

ARBEITSBERICHTE DES INSTITUTS FÜR MATHEMATISCHE MASCHINEN UND DATENVERARBEITUNG (INFORMATIK)

FRIEDRICH ALEXANDER UNIVERSITÄT ERLANGEN NÜRNBERG

**HERAUSGEBER: H. Billing, W. Händler, U. Herzog,
F. Hofmann, K. Leeb, P. Mertens, H. Müller, G. Nees,
H. Niemann, D. Seitzer, H. J. Schneider**

ON RESOLUTIONS OF STEINER SYSTEMS

Thomas Beth

ARBEITSBERICHTE DES INSTITUTS FÜR MATHEMATISCHE MASCHINEN UND DATENVERARBEITUNG (INFORMATIK)

FRIEDRICH ALEXANDER UNIVERSITÄT ERLANGEN NÜRNBERG

HERAUSGEBER : H. Billing, W. Händler, U. Herzog,
F. Hofmann, K. Leeb, P. Mertens, H. Müller, G. Nees,
H. Niemann, D. Seitzer, H. J. Schneider

ON RESOLUTIONS OF STEINER SYSTEMS

Den Naturwissenschaftlichen Fachbereichen
der Friedrich-Alexander-Universität Erlangen-Nürnberg

zur

Erlangung des Doktorgrades

vorgelegt

von

Thomas Beth

aus

Hannover

Als Dissertation genehmigt von den Naturwissenschaftlichen Fach-
bereichen der Universität Erlangen-Nürnberg

Tag der mündlichen Prüfung:

15. Februar 1978

Vorsitzender der Promotionskommission:

Professor Dr. E. Schweizer

Erstberichterstatte:

Professor Dr. K. Jacobs

Zweitberichterstatte:

Professor Dr. A. Barlotti

DEUTSCHE ZUSAMMENFASSUNG

Einem Vorschlag von D.K. Ray-Chaudhuri folgend wird in dieser Dissertation die Frage der Auflösbarkeit von Steiner Systemen untersucht.

Ein Steiner System $S_1(t, k, v)$ mit den Parametern $t, k, v \in \mathbb{N}$ ist ein System von k -Teilmengen (Blöcken) einer Menge von v Elementen (Punkten) mit der Eigenschaft, daß es zu je t verschiedenen Punkten genau einen Block gibt, der diese Punkte enthält. Ein Steiner System $S_1(t, k, v)$ heißt t' -auflösbar, wenn die Menge der Blöcke so zerlegt werden kann, daß jede Komponente der Zerlegung ein Steiner System $S_1(t', k, v)$ bildet.

Ein historisches Beispiel ist das Kirkman'sche Schulmädchenproblem, d.h. das Problem 1-auflösbare Steiner Systeme $S_1(2, 3, v)$ zu konstruieren. Aus der Lösung dieses Problems durch Ray-Chaudhuri und Wilson im Jahre 1970 ergab sich natürlicherweise die Fragestellung nach der t' -Auflösbarkeit anderer Steiner Systeme $S_1(t, k, v)$.

In Kapitel 3 dieser Arbeit werden solche Systeme für $t' < t \leq k \in \{2, 3, 4\}$ vorgestellt. Dabei stellt sich heraus, daß t' -Auflösungen mit transitiven Automorphismen eine besondere Rolle spielen.

In Kapitel 4 wird das Problem untersucht, 3-auflösbare Steiner Systeme $S_1(4, 4, v)$ zu konstruieren, d.h. das System $S_1(4, 4, v)$ in $v-3$ Steiner Systeme $S_1(3, 4, v)$ zu partitionieren. Nach Ray-Chaudhuri bietet sich als bisher einziges das folgende, von Schreiber und Wilson für andere Parameter erfolgreich eingesetzte Verfahren an: Als Punktmenge X nehme man eine abelsche Gruppe G der Ordnung $v-3$ zusammen mit drei weiteren Symbolen, die unter der Addition in G fest verbleiben.

Sei $\mathcal{B}_0 \subset \binom{G}{4}$ das System der 4-Teilmengen $\{x,y,z,u\}$ von G mit $x+y+z+u = 0$. Eine Partition $\{\mathcal{C}_g \mid g \in G\}$ von $\binom{X}{4}$, so daß $\mathcal{B}_0 \subset \mathcal{C}_0$ und $(X, \mathcal{C}_0)$ ein $S_1(3,4,v)$ ist, heißt eine SW_3 -Auflösung über G . Dann gilt der

Satz: Sei G eine endliche abelsche Gruppe. Dann gibt es keine SW_3 -Auflösung über G .

Dieses Ergebnis entspricht den bisher bekannten Resultaten für $v = 8, 10, 14$.

Der Beweis benutzt ein Argument über abzählbar unendliche Gruppen, für die die obigen Betrachtungen ebenfalls gelten - mit der einzigen Modifikation, daß die Systeme $S_1(3,4,v)$ für $v = \sum_{i=0}^{\infty} 2^i$ definiert werden müssen. Dann gilt der

Satz: Sei G eine abelsche Gruppe mit $6 \in \text{Aut } G$. Eine SW_3 -Auflösung über G existiert genau dann, wenn G torsionsfrei ist.

In Kapitel 5 wird eine Verallgemeinerung dieser Methoden vorgestellt, um k -Auflösungen der Steiner Systeme $S_1(k+1, k+1, \sum_{i=0}^{\infty} 2^i)$ zu konstruieren.

ACKNOWLEDGEMENTS

The research for this dissertation was initiated during the academic year 1973/74 when holding a scholarship from Deutscher Akademischer Austausch Dienst (DAAD) I had the opportunity to study at the Ohio State University. I am grateful to Professor D.K. Ray-Chaudhuri for guiding my first steps in this field and for suggesting the subject of this dissertation. I also wish to thank Professor R.M. Wilson for many stimulating discussions.

I am indebted to Professor K. Leeb under whose guidance I have had the opportunity to work since 1974. Without his support and valuable ideas I would not have been able to succeed in finishing this dissertation.

My sincere thanks are due to Professor K. Jacobs for his advice and encouragement during the last five years.

Finally I wish to express my gratitude to my colleagues M. Becker, V. Strehl, K.S. Vijayan for their help and patience during the preparation of this paper and Mrs. C. Matejka for her excellent typing of the manuscript.

CONTENTS:

CHAPTER 1	: INTRODUCTION	1
CHAPTER 2	: BASIC CONCEPTS	6
2.1	: Incidence Structures	6
2.2	: Graphs	9
2.3	: t-Designs	11
2.4	: Resolutions	19
CHAPTER 3	: RESOLUTIONS OVER FINITE FIELDS	24
3.1	: 1-Resolutions of $S_1(3,3,v)$	24
3.2	: 2-Resolutions of $S_1(3,3,v)$	26
3.3	: Double Resolvability	29
3.4	: Some Resolutions for Quadruples	34
CHAPTER 4	: PARTITIONING ALL QUADRUPLES INTO STEINER QUADRUPLE SYSTEMS	39
4.1	: Introduction	39
4.2	: Definition and Necessary Conditions	42
4.3	: A Lifting Theorem	70
4.4	: Admissible Colourings over $\mathbb{Z}[\frac{1}{6}]$	75
CHAPTER 5	: HIGHER RESOLUTIONS	93
5.1	: Definitions	93
5.2	: The Existence of SW_k -Resolutions	95
NOTATIONS		98
REFERENCES		100

CHAPTER 1: INTRODUCTION

In 1852 Steiner [49] published a paper entitled "Combinatorische Aufgabe" in Crelle's Journal für die Reine und Angewandte Mathematik, where he reports that studying double-tangents of curves of 4th degree leads to a problem which reads

"Welche Zahl, N , von Elementen hat die Eigenschaft, daß sich die Elemente so zu dreien ordnen lassen, daß je zwei in *einer*, aber *nur in einer* Verbindung vorkommen?"

Translated to modern terminology Steiner asks for which numbers N there exists a 2-design $S_1(2,3,N)$.

This question was answered by Reisz in 1857 [44].

Quoting M. Hall Jr. [27] "these writers were not aware that the problem had been posed and solved by Kirkman [32] in 1847."

In the very same paper Kirkman proposed a further problem, referred to by Cayley [15] as follows:

"The problem was proposed by Mr. Kirkman, and has, to my knowledge, excited some attention in the form 'To make a school of fifteen young ladies walk together in threes every day for a week so that each two may walk together'. It will be seen from the text that I am uncertain as to the existence of a solution to the further problem suggested by Mr. Sylvester, 'to make the school walk every week in the quarter so that each three may walk together'."

In modern terms it is Kirkman's Problem to construct a 1-resolvable 2-design $S_1(2,3,15)$ while Sylvester actually is asking for a doubly resolvable $S_1(3,3,15)$.

A t -design $S_1(t, k, v)$ with positive integers t, k and v is a system of k -subsets, called blocks, of a set of v points, such that any collection of t points is contained in a unique block.

A t -design $S_1(t, k, v)$ is called t' -resolvable if the class of blocks can be partitioned such that each part forms a t' -design $S_1(t', k, v)$.

In 1850 Kirkman [33] generalized his problem of fifteen school girls by asking for the existence of 1-resolvable systems $S_1(2, 3, 6n+3)$ for any $n \in \mathbb{N}$.

This problem was later (cf. Netto [40]) called Kirkman's School Girl Problem and it should take more than 100 years for a complete solution. The problem proposed by Sylvester has been considered by Cayley and Kirkman:

Cayley [15] disproved that $S_1(3, 3, 7)$ is 2-resolvable and Kirkman [32] showed that for $v = 9$ $S_1(3, 3, v)$ can be partitioned into 2-designs each of which is 1-resolvable. 3-designs $S_1(3, 3, v)$ with this property are said to be doubly-resolvable.

In the later parts of the above paper [49] Steiner asks for the existence of systems $S_1(3, 4, v)$, $S_1(4, 5, v)$, $S_1(5, 6, v)$ and $S_1(6, 7, v)$.

For this reason nowadays any t -design $S_1(t, k, v)$ is called a Steiner System, while the systems $S_1(2, 3, v)$ are called Steiner triple systems $STS(v)$ and the systems $S_1(3, 4, v)$ are called Steiner quadruple systems $SQS(v)$.

It was again Kirkman [32] who constructed $SQS(2^n)$ for every integer $n \geq 2$.

In the following years much work was done on Steiner triple systems and not much on Steiner quadruple systems nor on more general Steiner systems or their resolvability.

In 1901 Netto [40] dedicated two chapters of his "Lehrbuch der Combinatorik" to the subject of Steiner triple systems.

A survey of the progress made in the theory of Steiner systems has been documented recently by Doyen and Rosa [24] (respectively Lindner and Rosa [36]).

It was not until the late 1930's that a substantial progress was achieved when Bose [11] published his famous paper "On the construction of balanced incomplete block designs".

He had been influenced by Fisher and Yates, cf. [24], who conceived the idea of 2-designs from the statistical point of view and developed necessary conditions and constructed several examples.

About the same time Peltesohn [41] proved the 1-resolvability of any $S_1(3,3,3n)$. While Bose's paper initiated an avalanche of probably thousands of publications dealing with the construction of special 2-designs and their use in the design of statistical experiments, Peltesohn's paper remained widely unknown. A subsequent paper by Peltesohn [42] and Witt's two famous papers on Mathieu groups [56] and on Steiner Systems [57] finally established the connections between group theory and the theory of t-designs. The close interrelation between groups and t-designs (generally speaking between groups and incidence structures) did become more and more important not only in geometry (cf. Baer [1]), but also in group theory, especially in the search for simple groups. An excellent presentation of this can be found in Lüneburg [37].

Therefore the modern theory of t-designs which very often is considered as a part of finite geometry, cf. Dembowski [16], does not only deal with the construction of t-designs but also is concerned with the investigation of their structure. A typically geometric approach of this type is the search for substructures whose properties are similar to those

of affine or projective spaces. Thus t -designs with parallelisms are of special interest.

The first progress in this direction was made in 1970 by Ray-Chaudhuri and Wilson [43] when they solved Kirkman's School Girl Problem.

Recently more attention is being given to the study of resolvability of t -designs in general.

Chapter 3 contains a short summary.

The most surprising result concerning resolvability is that by Baranyai [3] in 1972, when he proved that each $S_1(k, k, n, k)$ is 1-resolvable. In 1976 Cameron [13] published a whole book on this topic. One of his main tools is the use of coding theory, connections of which with t -designs, geometry and group theory had been known before (cf. Sloane [48], Cameron - van Lint [14]).

At this point it may be remarked that geometric properties of t -designs which are related to certain codes (cf. van Lint [52], MacWilliams and Sloane [38]), also are of practical use in encoding and decoding procedures. Another application of t -designs in computer science arises in the design of filing schemes, where especially t' -resolvable t -designs and their automorphism groups are of some interest [8].

The present paper deals with the construction and classification of certain t' -resolvable t -designs. In analogy with Cameron [13] only t' -resolutions of t -designs with certain algebraic properties are considered:

In this case it is assumed that the t' -resolvable $S_1(t, k, v)$ has a group of automorphisms acting transitively on the parts of the resolution.

Several examples of t' -resolutions of $S_1(t,k,v)$'s for $t' < t \in \{2,3,4\}$, $k \in \{3,4\}$ are given in chapter 3.

Chapter 4 is concerned with the problem to construct a 3-resolution of $S_1(4,4,v)$, i.e. a partition of the class of all 4-subsets of a set of v elements into $v-3$ SQS(v)'s. Following a successful idea of Schreiber [45] and Wilson [54], Ray-Chaudhuri suggested to proceed as follows: For the point set X of v elements take an abelian group G of order $v-3$ and three extra symbols, which are invariant under the addition of G . Let $\beta_0 \subset \binom{G}{4}$ be the system of all 4-subsets $\{x,y,z,u\}$ with $x+y+z+u = 0$. If $|G| \equiv 1 \pmod{2}$, $\{\beta_0 + g \mid g \in G\}$ is a partition of $\binom{G}{4}$. Construct a partition $\{\alpha_0 + g \mid g \in G\}$ of $\binom{X}{4}$ such that $\beta_0 \subset \alpha_0$ and the blocks of α_0 form an SQS(v). This is called an SW_3 -resolution over G . The main result of chapter 4 is

Theorem: Let G be a finite abelian group. Then there is no SW_3 -resolution over G .

This negative result corresponds with the negative results for $v = 8, 10$ and 14 , which had been known before, cf. Lindner-Rosa [36]. The proof of this theorem makes use of an argument on countably infinite groups G for which the above considerations apply. The only modification required is that the Steiner Quadruple Systems are defined over a point set of cardinality $\aleph_0$. Then the following theorem holds:

Theorem: Let G be an abelian group with $6 \in \text{Aut } G$. There exists a SW_3 -resolution of $\binom{X}{4}$ iff G is torsionfree.

Chapter 5 presents a method which generalizes these partitions to construct k -resolutions of the complete $(k+1)$ -design over a point set of cardinality $\aleph_0$.

CHAPTER 2: BASIC CONCEPTS

2.1 Incidence Structures.

The structures mentioned in the preceding introduction were special examples of incidence structures which shall be defined in the following.

2.1.1 Definition: Let X and $\mathcal{B}$ be non-empty sets, $X \cap \mathcal{B} = \emptyset$. Then the triple $\mathcal{I} = (X, \mathcal{B}, I)$ is called an incidence structure, if $I \subseteq X \times \mathcal{B}$.

The elements $x \in X$ are called points, the elements $B \in \mathcal{B}$ are called blocks and the elements $(x, B) \in I$ are called flags. If $(x, B) \in I$, it is said that "the point x is on the block B " or " B contains x " or " x and B are incident" etc. The set I is called the incidence relation of $\mathcal{I}$.

2.1.2 Remark: This definition of an incidence structure, cf. Dembowski [16], is so general that at this point no further properties can be derived. The following definition shall provide a method to classify incidence structures in the following sections.

2.1.3 Definition: Let $\mathcal{I} = (X, \mathcal{B}, I)$ and $\mathcal{J} = (Y, \mathcal{A}, J)$ be two incidence structures. A homomorphism of $\mathcal{I}$ into $\mathcal{J}$ is a mapping $\phi : X \cup \mathcal{B} \rightarrow Y \cup \mathcal{A}$ such that $\phi(X) \subseteq Y$, $\phi(\mathcal{B}) \subseteq \mathcal{A}$ and for each $p \in X$ and each $B \in \mathcal{B}$ $(p, B) \in I$ implies $(\phi(p), \phi(B)) \in J$.

ϕ is called an epimorphism of $\mathcal{I}$ onto $\mathcal{J}$, if $\phi(X) = Y$ and $\phi(\beta) = \mathcal{O}$.

ϕ is called an isomorphism, if it is a bijective epimorphism the inverse of which is an epimorphism.

$\mathcal{I}$ and $\mathcal{J}$ are called isomorphic, if there exists an isomorphism of $\mathcal{I}$ onto $\mathcal{J}$.

An automorphism is an isomorphism of an incidence structure onto itself.

2.1.4 Observation: Let $\mathcal{I} = (X, \beta, I)$ be an incidence structure. The automorphisms of $\mathcal{I}$ form a group, $\text{Aut}(\mathcal{I})$.

2.1.5 Notation: $\text{Aut}(\mathcal{I})$ is called the automorphism group of $\mathcal{I}$.

A subgroup $H \leq \text{Aut}(\mathcal{I})$ is called a group of automorphisms of $\mathcal{I}$.

While the notion of isomorphism can be applied to recognize "similar" systems, on the other hand, it is important to classify these incidence structures by numerical properties of the incidence relation. For this purpose one more definition has to be made.

2.1.6 Definition: Let $\mathcal{I} = (X, \beta, I)$ be an incidence structure. Let $x \in X$ be point of $\mathcal{I}$. Then $(x) := \{B \in \beta \mid (x, B) \in I\}$ is called the pencil in x . Let $B \in \beta$ be a block of $\mathcal{I}$. Then $(B) := \{x \in X \mid (x, B) \in I\}$ is called the trace of B .

For further investigations only those incidence structures shall be considered, which fulfil some finiteness conditions.

2.1.7 Definition: Let $\mathcal{J} = (X, \mathcal{B}, I)$ be an incidence structure. $\mathcal{J}$ is called finite, if $|X|, |\mathcal{B}| < \infty$. $\mathcal{J}$ is called semifinite, if for each $B \in \mathcal{B}$ $|B| < \infty$.

2.1.8 Definition: An incidence structure $(X, \mathcal{B}, I)$ is called simple, if the mapping

$$(\cdot) : \mathcal{B} \longrightarrow 2^X$$

given by the trace is injective.

2.1.9 Remark: A simple incidence structure $\mathcal{J}$ is uniquely described by a pair $(X, \mathcal{B})$ where X is the point set, $\mathcal{B}$ the block set, and $\mathcal{B} \subseteq 2^X$ and incidence is given by inclusion.

2.1.10 Observation: Let $\mathcal{J}$ be a simple incidence structure. Let $\phi \in \text{Aut}(\mathcal{J})$. Then ϕ is uniquely determined by its restriction to the point set of $\mathcal{J}$.

2.1.11 Definition: Let $\mathcal{J} = (X, \mathcal{B}, I)$ and $\mathcal{J}' = (X', \mathcal{B}', I')$ be incidence structures. $\mathcal{J}'$ is called a substructure of $\mathcal{J}$ if $X' \subseteq X$, $\mathcal{B}' \subseteq \mathcal{B}$ and $I' = I \cap (X' \times \mathcal{B}')$.

2.2 Graphs

2.2.1 Definition: Let $\mathcal{G} = (V, E)$ be a simple semifinite incidence structure such that for each $e \in E$ $|e| = 2$. Then $\mathcal{G}$ is called a simple graph. Each element $v \in V$ is called a vertex of $\mathcal{G}$ and each element $e \in E$ is called an edge of $\mathcal{G}$.

A substructure of $\mathcal{G}$ is called a subgraph of $\mathcal{G}$ if it is a simple graph.

Let $S \subseteq V$ be a set of vertices. The subgraph of $\mathcal{G}$ generated by S is the subgraph $(S, E(S))$ where $E(S) = \{e \in E \mid e \subseteq S\}$.

In the further investigations it is no restriction to make the following agreement:

2.2.2 Agreement: Henceforth only simple graphs shall be considered.

Thus they will only be referred to as graphs.

2.2.3 Example: Let X be a set with at least two elements. The graph $(X, \binom{X}{2})$ is called the complete graph on X . If $|X| = n < \infty$, it is denoted by K_n :



2.2.4 Definition: Let $\mathcal{G} = (V, E)$ be a graph. Let $s, t \in V$. For $n \in \mathbb{N}_0$ a path of length n in $\mathcal{G}$ from s to t is a sequence $(s=v_0, \dots, v_n=t)$ such that for each $i \in \mathbb{N}_n$ $\{v_{i-1}, v_i\} \in E$. The path is called a polygon of size n if $s = t$ and for $i, j \in \mathbb{N}_n$ $i \neq j$ implies $v_i \neq v_j$. s and t are said to be connected, if for some $n \in \mathbb{N}_0$ there exists a path of length n from s to t in $\mathcal{G}$.

2.2.5 Remark: Connectedness is an equivalence relation on V . The subgraphs generated by the equivalence classes are called the components of $\mathcal{G}$.

2.2.6 Definition: A 2-way-path-graph is a graph isomorphic to the graph $(\mathbb{Z}, \beta)$ where $\beta = \{\{z, z+1\} \mid z \in \mathbb{Z}\}$.

2.2.7 Definition: Let $k \in \mathbb{N}$ and $G = (V, E)$ be a graph. A map $\phi : V \rightarrow \mathbb{N}_k$ is called a vertex- k -colouring if for $\{x, y\} \in E$ $\phi(x) \neq \phi(y)$. A mapping $\eta : E \rightarrow \mathbb{N}_k$ is called an edge- k -colouring, if for $e, e' \in E$ $|e \cap e'| = 1$ implies $\eta(e) \neq \eta(e')$.

2.3 t-Designs

Most of the structures later investigations are dedicated to, are t-designs which shall be introduced here:

2.3.1 Definition: Let X be a non-empty set, $\lambda, t, k \in \mathbb{N}$ and $t \leq k \leq |X|$.

A semifinite incidence structure $\mathcal{D} = (X, \mathcal{B}, I)$ is called a t-design

$S_\lambda(t, k, |X|)$ if

(i) for each $B \in \mathcal{B}$ $|B| = k$

(ii) for each $T \in \binom{X}{t}$ there are exactly λ blocks $B_1, \dots, B_\lambda \in \mathcal{B}$

such that for each $i \in \mathbb{N}_\lambda$ $T \subseteq (B_i)$.

2.3.2 Agreement: Hereafter, only simple t-designs will be considered.

At this point it has to be mentioned that most of the work so far has been confined to t-designs over finite sets. As the coming chapters will show, interesting properties can be developed for t-designs over infinite sets.

2.3.3 Examples:

(i) Let $k \in \mathbb{N}$ and X be a set of at least k elements. Then $(X, \binom{X}{k})$ is an $S_1(k, k, |X|)$, called the complete k-design on X .

(Hence the complete graph on X can be considered as a 2-design $S_1(2, 2, |X|)$).

(ii) Let q be a prime power, V_q^2 the 2-dimensional vector space over $GF(q)$ and $\mathcal{L}$ the class of all lines in V_q^2 . Then $(V_q^2, \mathcal{L})$ is an $S_1(2, q, q^2)$ (in other words $AG(2, q)$ is an $S_1(2, q, q^2)$).

(iii) Let q be a prime power, $n, k \in \mathbb{N}$, where $k < n$. Let V_q^n be the n -dimensional vector space over $GF(q)$ and Σ_k be the class of all k -dimensional (affine) subspaces of V_q^n . Then

$$(V_q^n, \Sigma_k) \text{ is an } S_\lambda(2, q^k, q^n)$$

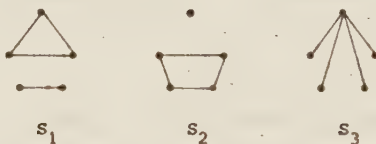
where $\lambda = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$.

(iv) Let q be a prime power. Then $PG(2, q)$ is an $S_1(2, q+1, q^2+q+1)$.

(v) Let $X = \mathbb{Z}_7$ and $\beta = \{\{1, 2, 4\} + g \mid g \in \mathbb{Z}_7\}$. Then (X, β) is an $S_1(2, 3, 7)$ and isomorphic to $PG(2, 2)$.

(vi) Let $X = \mathbb{Z}_{13}$ and $\beta = \{\{0, 1, 3, 9\} + g \mid g \in \mathbb{Z}_{13}\}$. Then (X, β) is an $S_1(2, 4, 13)$ and isomorphic to $PG(2, 3)$.

(vii) Let $X = \binom{N_5}{2}$, i.e. the edge set of K_5 . The following subgraphs of K_5 are defined:



Let β be the class of subgraphs of K_5 isomorphic to one of S_1 , S_2 or S_3 . Then (X, β) is an $S_1(3, 4, 10)$.

(viii) Let $X = V_2^n$ be the n -dimensional vector space over $GF(2)$, where $n \in \mathbb{N}$, $n \geq 2$.

Let $\mathcal{E}$ be the class of planes in V_2^n . Then $(X, \mathcal{E})$ is an $S_1(3, 4, 2^n)$.

(ix) The Golay Codes provide an example of the connections between codes and t -designs:

Let $\mathcal{C} \subset V_2^{24}$ be the $(12, 24)$ extended Golay Code.

For $\underline{\omega} \in \mathcal{C}$, $\underline{\omega} = (\omega_1, \dots, \omega_{24})$, let

$$B_{\underline{\omega}} := \{i \in \mathbb{N}_{24} \mid \omega_i = 1\}.$$

With $\mathcal{B} = \{B_{\underline{\omega}} \mid \underline{\omega} \in \mathcal{C}, |B_{\underline{\omega}}| = 8\}$ ($(\mathbb{N}_{24}, \mathcal{B})$ is an $S_1(5, 8, 24)$, cf. Sloane [48]. This 5-design has first been constructed by Witt [57] as an application of the Mathieu group $\mathcal{M}_{24}$.

Some conditions necessary for the existence of t -designs are stated without proof.

2.3.4 Definition: Let $\mathcal{D} = (X, \mathcal{B})$ be an $S_{\lambda}(t, k, |X|)$ and $p \in X$. Then

$\mathcal{D}_p := (X \setminus \{p\}, \mathcal{B}_p)$ where

$$\mathcal{B}_p := \{B \setminus \{p\} \mid p \in B \in \mathcal{B}\}$$

is called the derivation of $\mathcal{D}$ at the point p .

2.3.5 Lemma: Let $\mathcal{D} = (X, \mathcal{B})$ be an $S_{\lambda}(t, k, |X|)$ where $t \geq 2$. Let $p \in X$.

Then the derivation $\mathcal{D}_p$ is an $S_{\lambda}(t-1, k-1, |X|-1)$.

2.3.6 Lemma: Let $\lambda, t, k, v \in \mathbb{N}$, $t \leq k \leq v$. If there exists an $S_{\lambda}(t, k, v)$ $(X, \mathcal{B})$ then

$$|\mathcal{B}| = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}.$$

2.3.7 Corollary: Let $\lambda, t, k, v \in \mathbb{N}$ as above. If there exists an $S_{\lambda}(t, k, v)$ then for each $0 \leq i \leq t-1$

$$\lambda \binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}.$$

Proofs of 2.3.5 - 2.3.7 can be found in Dembowski [17].

In the further considerations the following t-designs play a major role:

2.3.8 Notation: (i) An $S_1(2,3,|X|)$ is called a Steiner Triple System on $|X|$ points, denoted by $STS(|X|)$.

(ii) An $S_1(3,4,|X|)$ is called a Steiner Quadruple System on $|X|$ points, denoted by $SQS(|X|)$.

2.3.9 Remark: For the origin of these names see Halder/Heise [28], pp. 238 - 239 . For further references see Doyen/Rosa [24] .

The following observations state those facts about STS's and SQS's which are used later.

2.3.10 Theorem: Let $v \in \mathbb{N}$. A necessary and sufficient condition for the existence of an $STS(v)$ is

$$v \equiv 1 \text{ or } 3 \pmod{6} \text{ and } v \geq 3 .$$

Proof: Hall [27] . #

3.2.11 Theorem: Let $v \in \mathbb{N}$. A necessary and sufficient condition for the existence of an $SQS(v)$ is

$$v \equiv 2 \text{ or } 4 \pmod{6} \text{ and } v \geq 4 .$$

Proof: The necessity is immediate since the derivation of an $SQS(v)$ is an $STS(v-1)$. The sufficiency was shown by Hanani [29] in a long and remarkable proof. #

2.3.12 Observation: The smallest $v \in \mathbf{N}$ for which a nontrivial $\text{STS}(v)$ exists therefore is $v = 7$. It is easily shown that - up to isomorphism - $\text{STS}(7)$ is unique.

The derivation of an $\text{SQS}(8)$ is an $\text{STS}(7)$, which in turn completely determines the $\text{SQS}(8)$ the derivation of which it is:

Let $(\mathbf{N}_7, \beta)$ be the $\text{STS}(7)$ obtained by derivation of an $\text{SQS}(8)$
 $(\mathbf{N}_7 \cup \{\infty\}, \bar{\beta})$.

By definition 2.3.4 $B \in \beta$ implies $B \cup \{\infty\} \in \bar{\beta}$. Thus the remaining blocks of $\bar{\beta}$ must be of the form $\bar{B} = \mathbf{N}_7 \setminus B$ for each $B \in \beta$.

Hence the $\text{SQS}(8)$ is unique up to isomorphism and hence isomorphic to $(V_2^3, \mathcal{C})$, cf. 2.3.3 (viii). In analogy with 2.3.3 (ix) it may be mentioned that the $\text{SQS}(8)$ corresponds to the extended Hamming code $(4, 8)$.

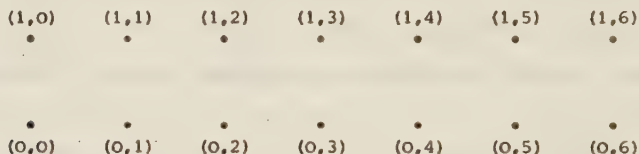
2.3.13 Fact: The $\text{SQS}(10)$ given in 2.3.3 (vii) is unique (up to isomorphism) and isomorphic to the Möbius plane of order 3. For references see Rosa/Lindner [36], p. 7 and Dembowski [16].

Although the method of difference sets proved to be very powerful in the construction of 2-designs $S_\lambda(2, k, v)$ (Bose [11], Dembowski [16] Wilson [53], [55]) for t -designs with $t \geq 3$, not too many similar methods seem to be known. A few examples of methods, a suitable generalization of which could lead to generalized difference methods for the construction of 3-designs, shall be given below.

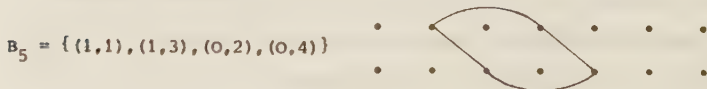
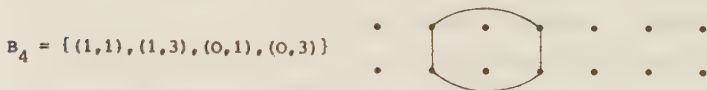
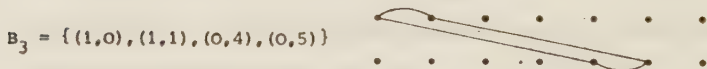
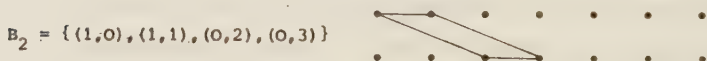
A first approach to treat 3-subsets with difference-quotient methods has been pointed out in [7] and will be used in chapter 3 several times. The following two constructions were made by the author in order to demonstrate the applicability of the methods of [7].

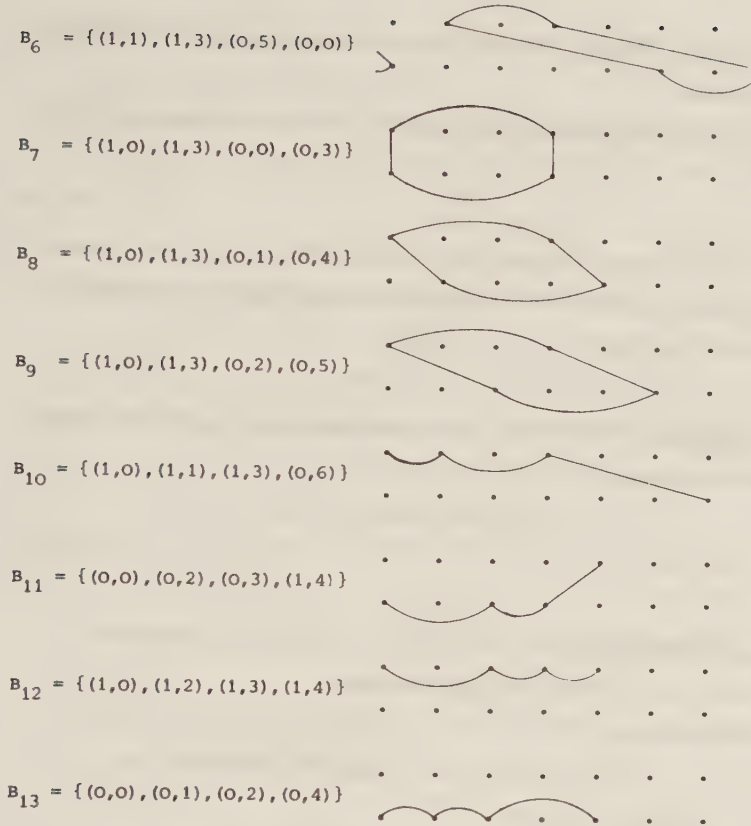
2.3.14 Construction: In order to construct an SQS(14) one has to construct $b = \frac{14 \cdot 13 \cdot 12}{4 \cdot 3 \cdot 2} = 91$ blocks, which have to contain every three elements out of 14 exactly once. The divisibility of 14 and 91 by 7 makes the question conceivable, whether this SQS(14) can be obtained from two copies of STS(7), each of which has 7 points and 7 blocks. In the following pictures such a solution is presented:

Let $X = \mathbb{Z}_2 \times \mathbb{Z}_7$, being interpreted as two rows of seven dots:



Let $\mathcal{B} = \{B_i + (0, g) \mid i \in \mathbb{N}_{13}, g \in \mathbb{Z}_7\}$ where for $i \in \mathbb{N}_{13}$ the B_i are given as follows:





Then (X, β) is an SQS(14).

Some remarks shall conclude this example:

(i) Realizing that $\{\mathbb{Z}_7, \{1, 2, 4\} + g \mid g \in \mathbb{Z}_7\}$ is the STS(7), cf. 2.3.3 (v), and recalling the construction of 2.3.12, the relation to STS(7) is clear from the blocks $B_{10}, \dots, B_{14}$.

(ii) The complete listing of all "base" blocks $B_1, \dots, B_{13}$ was carried out in order to show the construction. Allowing the multiplication by

elements of $GF(7)^*$ in each component, the number of base blocks can be reduced.

(iii) The automorphism group $\text{Aut}(X, \beta)$ is known, Mendelsohn/Hung [39].

The next example will show a construction where an $S_1(3,5,26)$ is built up from two copies of an $S_1(2,4,13)$ the properties of which have to be mentioned first.

2.3.15 Fact: An $S_1(2,4,13)$ is uniquely determined (up to isomorphism) and isomorphic to $PG(2,3)$, respectively to

$$(\mathbb{Z}_{13}, \{ \{0,1,3,9\} + g \mid g \in \mathbb{Z}_{13} \})$$

cf. 2.3. (vi).

2.3.16 Construction: Let $G = \mathbb{Z}_2 \times \mathbb{Z}_{13}$. Since 2 is a primitive element mod 13, define blocks as follows:

For $\alpha \in \{0,1,2,3\}$ let

$$B_\alpha = \{ (0,0), (0,2^\alpha), (0,2^{\alpha+4}), (0,2^{\alpha+8}), (1,0) \}.$$

For $\beta \in \{0,1,2,3,4,5\}$ let

$$C_\beta = \{ (0,0), (0,2^\beta), (0,2^{\beta+6}), (1,2^{\beta+4}), (1,2^{\beta+10}) \}.$$

Define $\mathcal{B} = \{ B_\alpha + g \mid \alpha \in \{0,1,2,3\}, g \in G \} \cup \{ C_\beta + g \mid \beta \in \{0,1,2,3,4,5\}, g \in G \}.$

Then $(G, \mathcal{B})$ is an $S_1(3,5,26)$.

The following remarks are to be made:

The priority of this solution is due to Hanani, (personal correspondence of the author with R.M. Wilson who pointed out this fact). In the meantime, Denniston [21] succeeded in constructing an $S_1(5,7,28)$ which, by 2.3.5, implies the existence of an $S_1(3,5,26)$.

2.4 Resolutions

As an analogue to classical geometry, where properties of parallelisms play a major role, cf. Dembowski [16], for t -designs similar properties are important:

2.4.1 Definition: Let X be a set and $t, t', k \in \mathbb{N}$ such that $t' < t \leq k \leq |X|$.

An $S_1(t, k, |X|)$ $(X, \mathcal{B})$ is called t' -resolvable if there exists a partition

$\{\mathcal{B}_i \mid i \in I\}$ of $\mathcal{B}$ such that for each $i \in I$ $(X, \mathcal{B}_i)$ is an $S_1(t', k, |X|)$.

The partition $\{\mathcal{B}_i \mid i \in I\}$ is then called a t' -resolution of $\mathcal{B}$ (resp.

$(X, \mathcal{B})$).

2.4.2 Remark: Let $\mathcal{D}$ be a t' -resolvable t -design $S_1(t, k, |X|)$, where $t' \geq 2$. Let $p \in X$. Then the derived design $\mathcal{D}_p$ is a $(t'-1)$ -resolvable $(t-1)$ -design $S_1(t-1, k-1, |X|-1)$. This follows immediately from 2.3.5.

2.4.3 Example: Let q be a prime power and $n \in \mathbb{N}$ such that $n \geq 2$. Then $AG(n, q)$ is a 1-resolvable $S_1(2, q, q^n)$.

2.4.4 Notation: In analogy with this geometric example the following notation is made:

Let $\{\mathcal{B}_i \mid i \in I\}$ be a 1-resolution of an $S_1(t, k, |X|)$ $(X, \mathcal{B})$. Then the $\mathcal{B}_i$ are called parallel classes.

2.4.5 Remark and Notation: With the help of these definitions Kirkman's School Girl Problem [33], which has been mentioned in the introduction,

can be stated exactly:

It is the problem to construct a 1-resolvable $STS(6t+3)$ for $t \in \mathbb{N}_0$.

For this reason a 1-resolvable $STS(v)$ is said to be a Kirkman system of order v , where $v \in \mathbb{N}$.

The Kirkman's School Girl Problem was affirmatively solved by Ray-Chaudhuri and Wilson [43]:

2.4.6 Theorem: Let $v \in \mathbb{N}$. A Kirkman system of order v exists iff $v \equiv 3 \pmod{6}$.

Later this theorem, as well as the following examples, will be made use of.

2.4.7 Example: Let $n \in \mathbb{N}$ be even. Let X be a set, $|X| = n$. Then the complete graph $K_n = (X, \binom{X}{2})$ considered as an $S_1(2,2,n)$ is 1-resolvable:

Let $X = \mathbb{Z}_{n-1} \cup \{\infty\}$, where ∞ is a symbol not in $\mathbb{Z}_{n-1}$ such that $\infty + g = \infty$ for each $g \in \mathbb{Z}_{n-1}$.

Let $\mathcal{B}_0 = \{\{x, -x\} \mid x \in \mathbb{Z}_{n-1} \setminus \{0\}\} \cup \{\{\infty, 0\}\}$.

Then $\{\mathcal{B}_0 + g \mid g \in \mathbb{Z}_{n-1}\}$ is a 1-resolution of $\binom{X}{2}$. In the sequel there will be several theorems proving this as a special case.

2.4.8 Remark: (i) Example 2.4.7 shows that in terms of graph theory

K_n can be 1-factorized for $n \equiv 0 \pmod{2}$, whence the term "1-factorization" will be defined later.

(ii) Example 2.4.7 shows a t '-resolution having a group of automorphisms acting on it.

2.4.9 Definition: Let $\{\beta_i \mid i \in I\}$ be a t '-resolution of an $S_1(t, k, |X|)$ (X, β) .

Let $\phi \in \text{Aut}(X, \beta)$. ϕ is called an automorphism of the t '-resolution

$\{\beta_i \mid i \in I\}$ of β if for each $j \in I$ $\phi(\beta_j) \in \{\beta_i \mid i \in I\}$.

If there is no danger of confusion sometimes it is said that the t '-resolvable $S_1(t, k, |X|)$ admits ϕ as an automorphism.

2.4.10 Example: From 2.4.7 it follows that $\mathbb{Z}_{n-1}$ operates as a group of automorphisms of the given 1-resolution of K_n .

2.4.11 Remark: General results on automorphism groups of t '-resolutions can be found in Beker [5], Beker/Piper [6].

Finally, the one important general theorem on 1-resolutions shall be mentioned.

In order to do so, a few more notations have to be introduced:

2.4.12 Definition: Let $\mathcal{H} = (X, \mathcal{A}, I)$ and $\mathcal{J} = (X, \mathcal{B}, J)$ be finite incidence structures on the same point set X . Then the sum $\mathcal{H} + \mathcal{J}$ of $\mathcal{H}$ and $\mathcal{J}$ is the incidence structure

$$\mathcal{H} + \mathcal{J} = (X, \mathcal{A} \cup \mathcal{B}, I \cup J).$$

2.4.13 Remark: (i) In 2.4.12 " $\dot{\cup}$ " denotes the well-known disjoint union of sets.

(ii) Thus the summation of finite incidence structures can be considered as commutative and associative.

2.4.14 Definition: A substructure $\mathbb{F} = (X, \mathcal{B}', I')$ of a finite incidence structure $\mathcal{H} = (X, \mathcal{B}, I)$ is called a 1-factor of $\mathcal{H}$ if $\{\{B\} \mid B \in \mathcal{B}'\}$ is a partition of X .

A family $(\mathbb{F}_1, \dots, \mathbb{F}_r)$ of 1-factors of $\mathcal{H}$ with $r \in \mathbb{N}$ is called a 1-factorization of $\mathcal{H}$ if

$$\sum_{i=1}^r \mathbb{F}_i = \mathcal{H}.$$

2.4.15 Notation: (i) Let $\mathcal{H} = (X, \mathcal{B}, I)$ be an incidence structure and $\mathbb{F} = (X', \mathcal{B}', I')$ a substructure of $\mathcal{H}$.

Then $b_{\mathcal{H}}(\mathbb{F}) := \mathcal{B}'$ denotes the block set of $\mathbb{F}$ in $\mathcal{H}$.

(ii) Let X be a finite set and α be an integer $0 \leq \alpha \leq |X|$.

Then let $\mathcal{H}_\alpha(X)$ denote the incidence structure $(X, \binom{X}{\alpha}, I)$, where $I \subset X \times \binom{X}{\alpha}$ is the canonical containment relation.

(Trivially $\mathcal{H}_\alpha(X)$ is an $S_1(\alpha, \alpha, |X|)$, but in this context mostly called the α -regular hypergraph on X).

After these preparations Baranyai's [3] celebrated theorem can be stated:

2.4.16 Theorem: Let $n, p, r \in \mathbb{N}$ and X be a set of cardinality n .

Let $(\alpha_1, \dots, \alpha_p) \in \{0, \dots, n\}^p$ and $(a_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq r}}$ be a $p \times r$ -matrix where for

$i \in \mathbb{N}_p$ and $j \in \mathbb{N}_r$ $a_{ij} \in \mathbb{N}_0$. There exists a 1-factorization $(F_1, \dots, F_r)$

of $\mathcal{H} = \sum_{i=1}^p \mathcal{K}_{\alpha_i}(X)$ with $|\beta_{\mathcal{K}}(\mathcal{K}_{\alpha_i}(X)) \cap \beta_{\mathcal{K}}(F_j)| = a_{ij}$ for each $i \in \mathbb{N}_p$

and $j \in \mathbb{N}_r$ iff

$$(i) \quad \sum_{i=1}^p \alpha_i a_{ij} = n$$

$$(ii) \quad \sum_{j=1}^r a_{ij} = \binom{n}{\alpha_i}.$$

Proof: Baranyai [3], Beth [9], Brouwer [12].

2.4.17 Corollary (Sylvester's conjecture): Let $m, k \in \mathbb{N}$, where $k > 1$.

Then $S_1(k, k, k \cdot m)$ is 1-resolvable.

2.4.18 Remark: For $k = 2$ the statement of 2.4.17 has been proved earlier, cf. 2.4.7.

For $k = 3$ this was proved by Peltesohn [41] in her dissertation as early as 1937.

Partial results for $k = 3$ and 1-resolutions with transitive automorphisms were obtained by Beth [7]. In the following chapters these constructions shall be studied in some more detail.

CHAPTER 3: RESOLUTIONS OVER FINITE FIELDS

3.1 1-Resolutions of $S_1(3,3,v)$.

By Baranyai's theorem it is clear that for each positive integer $v \equiv 0 \pmod 3$ the trivial complete 3-design $S_1(3,3,v)$ can be resolved into $S_1(1,3,v)$'s.

The method used by Baranyai [3] - although combinatorially very interesting - does not use any structure of the underlying set.

As already pointed out in the introduction for some applications, cf. Beth - Vijayan [8], it is useful to refer to algebraic or geometric properties of the point set of the t -design in consideration.

One such procedure shall be presented here:

3.1.1 Observation: Let $q \equiv -1 \pmod 6$ be a prime power. Let $GF(q) \cup \{\infty\}$ be coordinatization of $PG(1,q)$. Let $\pi \in PGL(2,q)$ be given by $\pi : x \mapsto -\frac{1+x}{x}$ for each $x \in GF(q) \cup \{\infty\}$. Then π is fixed-point-free of order 3.

3.1.2 Theorem: Assume the notations of 3.1.1. Let $\mathcal{O} = \{A_i \mid 1 \leq i \leq \frac{q+1}{3}\}$ be the partition of $PG(1,q)$ into orbits of $\langle \pi \rangle$.

Let ω be a primitive element of $GF(q)$ and $H := \{\omega^j \mid 1 \leq j \leq \frac{q-1}{2}\}$.

Then

$$\{\lambda \mathcal{O} + g \mid \lambda \in H, g \in GF(q)\}$$

is a 1-resolution of $S_1(3,3,q+1)$.

Proof: Beth [7] $\neq$

3.1.3 Remark: Similar constructions for each prime power $q \not\equiv 0 \pmod{3}$ are given in Beth [7]. In all these cases the blocks A of the initial system $\mathcal{O}$ have the property that if they are contained in $GF(q)$ then

$$(O-\Sigma) \quad \prod_{x \in A} x = 1.$$

In the construction 3.1.2 this is trivially true for each block A_i , $1 \leq i \leq \frac{q+1}{3}$.

The property $(O-\Sigma)$ appears in many other constructions: Applied to the additive group $\mathbb{Z}_{2n-1}$ the blocks $\{x, y\}$ with

$$x+y = 0$$

form the essential part of the 1-resolution of $S(2, 2, 2n)$ given in 2.4.7.

If $q = 3^n$ for some $n \in \mathbb{N}$, a construction for a 1-resolution of $S_1(3, 3, 3^n)$ is given in [7], which shall not be repeated here, since Denniston [18] has a more general solution.

It is clear that the construction of 3.1.2 can be generalized to the field $\mathbb{Q}$ if one assumes $H := \{q \in \mathbb{Q} \mid q > 0\}$.

Further examples of applications of the property $(O-\Sigma)$ will be shown in the next section.

3.2 2-Resolutions of $S_1(3,3,v)$.

This section deals with the problem of partitioning the class of blocks of complete 3-designs $S_1(3,3,v)$ into STS(v)'s.

While Baranyai's theorem guarantees the existence of 1-resolutions whenever the cardinalities fulfil the necessary numerical conditions, the situation is not so simple even for 2-resolutions of $S_1(3,3,v)$.

3.2.1 Lemma: (i) Let $v \in \mathbb{N}$ and X be a set of cardinality v . $(X, \binom{X}{3})$ is 2-resolvable iff there exists a family $(\beta_i)_{i \in \mathbb{N}_{v-2}}$ of disjoint subclasses of $\binom{X}{3}$ such that for each $i \in \mathbb{N}_{v-2}$ (X, β_i) is an STS(v).
(ii) $S_1(3,3,7)$ is not 2-resolvable.

Proof: (i) is trivial.

(ii) It was shown by Cayley [15] that for a 7-set X the maximal number of pairwise disjoint subclasses $\beta_i \subset \binom{X}{3}$, such that each (X, β_i) is an STS(7), is 2. From (i) it follows that $S_1(3,3,7)$ is not 2-resolvable. #

3.2.2 Remark: From 3.2.1 (i) it follows that the numerical conditions 2.3.10 do not assure the existence of a 2-resolution of $S_1(3,3,v)$, while it is trivial to observe that 3.2.1 is not a real condition on v since $v-2$ always is an integer.

Therefore, constructions for 2-resolutions of $S_1(3,3,v)$'s are presently known only for certain families of parameters $v \in \mathbb{N}$.

The constructions, which are most interesting from the algebraic point of view, are due to Schreiber [45] and Wilson [54]. A complete summary of the general constructions for the problem of 2-resolvability can be found in Teirlinck [51].

3.2.3 Theorem (Schreiber-Wilson): The $S(3,3,v)$ is 2-resolvable if for every prime divisor p of $v-2$ the order of $-2 \bmod p$ is congruent to $2 \bmod 4$.

Proof: A complete proof can be found in [45] or [54]. Anticipating the later chapters it is useful to present the methods of Schreiber and Wilson. The proof will be carried out for the simpler case when $v-2$ is a prime:

Let $v \equiv 1, 3 \bmod 6$ be a positive integer, such that $p = v-2$ is a prime.

Let $\mathcal{Q}_0 := \{(x, y, z) \in \binom{\text{GF}(p)}{3} \mid x+y+z = 0\}$.

Observe that exactly those pairs $\{x, y\} \in \binom{\text{GF}(p)}{2}$ are not contained in any block of $\mathcal{Q}_0$, which are of the form $x+2y = 0$ or $2x+y = 0$.

Since $p \equiv 1, 5 \bmod 6$, each non zero element $x \in \text{GF}(p)^*$ is contained in exactly two such pairs: a) $\{-\frac{1}{2}x, x\}$ and b) $\{x, -2x\}$.

Let $\Gamma = (V, \mathcal{E})$ be the graph with vertex set V , the set $\text{GF}(p)^*$ of non-zero elements of $\text{GF}(p)$, and with edge set $\mathcal{E}$ consisting of the pairs of type a) or b). Then Γ is the union of disjoint polygons of length m , where $m = \min\{\ell \mid \ell \in \mathbb{N}, (-2)^\ell \equiv 1 \bmod p\}$, i.e. $m = \text{ord}_p(-2)$.

If m is even, there is an edge-2-colouring of Γ : Let $\{\alpha, \beta\}$ be a set of symbols disjoint from $\text{GF}(p)$ and

$$c : \mathcal{E} \longrightarrow \{\alpha, \beta\}$$

be such a 2-colouring of the edges of Γ .

Define $\mathcal{C}_0 := \{E \cup \{c(E)\} \mid E \in \mathcal{E}\}$. Then each pair $\{x, y\} \in \binom{\text{GF}(p)}{2}$ with $x + 2y = 0$ or $2x + y = 0$ is contained in a unique block of $\mathcal{C}_0$. Furthermore, each pair $\{\alpha, x\}$ and $\{\beta, x\}$ for $x \in \text{GF}(p)^*$ occurs in a unique block of $\mathcal{C}_0$.

Let $\mathcal{B}_0 := \mathcal{C}_0 \cup \{\{\alpha, \beta, 0\}\}$. Then $(\text{GF}(p) \cup \{\alpha, \beta\}, \mathcal{B}_0)$ is an $S_1(2, 3, p+2)$. It is now immediate that $\{\mathcal{C}_0 + g \mid g \in \text{GF}(p)\}$ is a partition of $\binom{\text{GF}(p)}{3}$. Thus $\{\mathcal{B}_0 + g \mid g \in \text{GF}(p)\}$ is a 2-resolution of $\binom{\text{GF}(p) \cup \{\alpha, \beta\}}{3}$ iff $\mathcal{C}_0 + g$ and $\mathcal{C}_0 + h$ are disjoint for all $h, g \in \text{GF}(p)$, $h \neq g$. This is true iff $\mathcal{C}_0$ and $\mathcal{C}_0 + g$ are disjoint for each $g \in \text{GF}(p)^*$.

Since a pair $\{x, -2x\}$ with $x \neq 0$ contained in a block, say $\{x, -2x, \alpha\}$, of $\mathcal{C}_0$, has only one translate, namely $\{x, -2x\} + x = \{2x, -x\}$, contained in a block of $\mathcal{C}_0$, $\mathcal{C}_0$ and $\mathcal{C}_0 + x$ are disjoint iff $\{2x, -x, \beta\} \in \mathcal{C}_0$. Thus $\mathcal{C}_0$ and $\mathcal{C}_0 + g$ are disjoint for each $g \in \text{GF}(p)^*$ iff the 2-colouring c of the edges of Γ is such that for each $x \in \text{GF}(p)^*$

$$c(\{x, -2x\}) = c(\{-x, 2x\}).$$

This is only possible, iff $m = \text{ord}_p(-2) \equiv 2 \pmod{4}$. #

3.2.4 Remark: The blocks of the initial system $\mathcal{B}_0$ of this 2-resolution fulfil again the condition (O- Σ) of section 3.1.

Since partitions fulfilling this condition apparently play a certain role, in the sequel they will be investigated in some more detail.

3.3 Double Resolvability.

After the sections 3.1 and 3.2 it is only natural to ask if 2-resolutions and 1-resolutions of an $S_1(3,3,v)$ can be constructed simultaneously in a "consistent" manner.

3.3.1 Definition: Let v be a positive integer, X be a set of cardinality v .

The complete 3-design $(X, \binom{X}{3})$ is said to be doubly-resolvable, if there exists a partition $\{\mathcal{B}_\lambda \mid \lambda \in \Lambda\}$ of $\binom{X}{3}$, such that for each $\lambda \in \Lambda$, $(X, \mathcal{B}_\lambda)$ is a 1-resolvable STS(v), i.e. each $\mathcal{B}_\lambda$ possesses a partition $\{\mathcal{B}_{\lambda,i} \mid i \in I\}$ such that for each $i \in I$ $(X, \mathcal{B}_{\lambda,i})$ is an $S_1(1,3,v)$.

3.3.2 Remark: An $S_1(3,3,v)$ is doubly resolvable iff it can be partitioned into Kirkman Systems of order v . Thus it is a necessary condition for the existence of a doubly-resolvable $S_1(3,3,v)$ that $v \equiv 3 \pmod{6}$.

There are only partial solutions of this problem:

$v = 9$	Kirkman [32]
$v = 3^n \ (n \in \mathbb{N})$	Denniston [18]
$v = 15$	Denniston [20]
$v = 33, 51, 75$	Schreiber [46]
$v = 51, 75, 105$	Denniston [22]
$v = 45, 135, 25 \cdot 3^n \ (n \in \mathbb{N})$	Denniston [23]

It is most likely that this list is incomplete.

3.3.3 Remark: Some considerations about the parameters involved will point out the difficulties and lead to a solution for $v = 33$:

Let $v \equiv 3 \pmod 6$ be a positive integer. If $S_1(3,3,v)$ is doubly resolvable, the $\binom{v}{3}$ blocks are partitioned into $(v-2)$ $S_1(2,3,v)$'s, each of which splits into $\frac{v-1}{2} S_1(1,3,v)$'s.

It would be interesting to compose the methods used in 3.1.2 and 3.2.3 in order to construct a double resolution. To be able to apply the method of Schreiber - Wilson for the first step of resolving an $S_1(3,3,v)$ into $S_1(2,3,v)$'s, the condition of 3.2.4 has to be fulfilled. The first two primes p such that $p \equiv 1 \pmod 6$ and $\text{ord}_p(-2) \equiv 2 \pmod 4$ are $p = 7$ and $p = 31$.

Since any system $S_1(2,3,9)$ is 1-resolvable the 2-resolution of $S_1(3,3,9)$ by Schreiber and Wilson trivially induces a double resolution.

Thus the next case $p = 31$ is the first interesting one for possibly applying the above methods:

3.3.4 Construction: Let $X = \text{GF}(31) \cup \{\alpha, \beta\}$ where $\{\alpha, \beta\}$ is a set of symbols disjoint from $\text{GF}(31)$. Let $\{\beta_0 + g \mid g \in \text{GF}(31)\}$ be the 2-resolution of $\binom{X}{3}$, which is given by Schreiber - Wilson, cf. 3.2.4. Since all the $S_1(2,3,33)$'s $(X, \beta_0 + g)$ are isomorphic, for the $S_1(3,3,33) (X, \binom{X}{3})$ to be doubly resolvable, it is necessary and sufficient that the $S_1(2,3,33) (X, \beta_0)$ is 1-resolvable.

(X, β_0) is 1-resolvable iff it splits into sixteen parallel classes. One parallel class $\beta_{0,0}$ of β_0 is canonically induced by the group of 3^{rd} roots of unity in $\text{GF}(31)$: Let θ be a primitive 3^{rd} root of unity, e.g. $\theta = 5$. Let $C_3 = \{1, \theta, \theta^2\}$ be the group of 3^{rd} roots of 1

in $\text{GF}(31)^*$. Let $\{x_i C_3 \mid i \in \mathbb{N}_{10}\}$ be the partition of $\text{GF}(31)^*$ into cosets of C_3 . It follows that $\beta_{\alpha 0} = \{x_i C_3 \mid i \in \mathbb{N}_{10}\} \cup \{0, \alpha, \beta\}$ is a parallel class in β_0 .

It remains to partition $\beta_0 \setminus \beta_{\alpha 0}$ into fifteen parallel classes.

Reconsidering the methods used in Beth [7] it is sufficient to find disjoint representatives of the orbits $\sigma_1, \dots, \sigma_{11}$ in which $\beta_0 \setminus \beta_{\alpha 0}$ is partitioned under the action of the group

$$\text{GF}(31)^{*2} := \{\pi_{a^2} \mid a \in \text{GF}(31)^*\}$$

where for each $a \in \text{GF}(31)$ π_{a^2} is given by

$$\pi_{a^2} : x \mapsto a^2 x \text{ for } x \in \text{GF}(31)$$

and

$$\pi_{a^2} : \rho \mapsto \rho \text{ for } \rho \in \{\alpha, \beta\}.$$

According to [7] the orbits can be characterized as follows: The blocks containing 0, α or β are recognized immediately. The remaining eight orbits can be characterized by four invariants, since -1 is a non-square in $\text{GF}(31)$ and thus the eight orbits come in four pairs of two, where the corresponding two orbits differ only by multiplication by -1. These invariants are, cf. [7] p. 120,

$$M_1 = \begin{bmatrix} 1 & 19 & 11 \\ 18 & 1 & 12 \\ 17 & 13 & 1 \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 1 & 28 & 2 \\ 10 & 1 & 20 \\ 16 & 14 & 1 \end{bmatrix}$$

$$M_3 = \begin{bmatrix} 1 & 26 & 4 \\ 6 & 1 & 24 \\ 8 & 22 & 1 \end{bmatrix}$$

$$M_4 = \begin{bmatrix} 1 & 3 & 27 \\ 21 & 1 & 9 \\ 23 & 7 & 1 \end{bmatrix}.$$

Here the elements of $GF(31)$ are identified with the set $N_{30} \cup \{0\}$.

With the help of these invariants it is clear that the following blocks fulfil the required property:

$$\begin{aligned} A_1 &= \{2, 6, 23\} & A_{-1} &= \{29, 25, 8\} \\ A_2 &= \{3, 4, 24\} & A_{-2} &= \{28, 27, 7\} \\ A_3 &= \{5, 10, 16\} & A_{-3} &= \{26, 15, 21\} \\ A_4 &= \{1, 11, 19\} & A_{-4} &= \{30, 20, 12\} \\ A_\alpha &= \{\alpha, 9, 13\} & A_\beta &= \{\beta, 22, 18\} \end{aligned}$$

$$A_0 = \{0, 14, 17\}.$$

For $i \in N_4$ one has $A_i = -A_{-i}$ and by applying the methods of [7]

it is clear that A_i is in the orbit represented by M_i .

Since $A_\alpha \cap GF(31) = -(A_\beta \cap GF(31))$ and $A_\alpha \cap GF(31) = \{9, 13\}$ fulfils

$2 \cdot 9 + 13 = 0$ it follows that $B_{01} := \{A_\lambda \mid \lambda \in \{-4, \dots, 0, \dots, 4, \alpha, \beta\}$ is

a parallel class in B_0 and $\{a^2 B_{01} \mid a^2 \in GF(31)^{\neq 2}\}$ is a partition of

$$B_0 \setminus B_{00}.$$

3.3.5 Remark: (i) This solution is due to the author, independent of that of Schreiber [private correspondence of the author]

(ii) There are three different solutions if one requires the above group of automorphisms for the generation of the double resolution.

(iii) There is - yet - no algorithm to construct the initial parallel class B_{01} for an infinite family of primes.

(iv) In this context the combinatorial composition theorems leading to double resolutions are not mentioned, cf. Teirlinck [51]

(v) For the sake of completeness it may be pointed out that the construction of the initial parallel class B_{01} can be reduced to con-

structing a proper Steiner function. Steiner functions have been introduced by Ferrero [25], [26], but his classifications [26] do not lead to any progress in the problem of double resolvability.

3.4 Some Resolutions for Quadruples.

Although from Baranyai's theorem it is clear that an $S_1(4,4,v)$ is 1-resolvable iff $v \equiv 0 \pmod{4}$, no algebraic resolution methods comparable to those of 3.1 - 3.2 seem to be known for this problem.

More is known about the 1- and 2-resolutions of $S_1(2,4,v)$'s and $S_1(3,4,v)$'s:

In the sequel of Ray-Chaudhuri-Wilson's solution of Kirkman's School Girl Problem [41], cf. 2.4.5, 2.4.6, Ray-Chaudhuri, Wilson and Hanani [31] proved the following

3.4.1 Theorem: Let $v \in \mathbb{N}$. A necessary and sufficient condition for the existence of a 1-resolvable $S_1(2,4,v)$ is that $v \equiv 4 \pmod{12}$.

The proof of theorem 3.4.1 is based on a proper composition of algebraic and purely combinatorial methods, a procedure which has been used before in the proof of Kirkman's School Girl Problem [41]. Almost exclusively algebraic were the methods used by Baker [2] in proving the following theorem.

3.4.2 Theorem: Let $m \in \mathbb{N}$, $X := (\text{GF}(2))^{2m}$ and $\mathcal{B}$ be the class of affine planes in $(\text{GF}(2))^{2m}$. Then the $S_1(3,4,2^{2m}) (X, \mathcal{B})$ can be partitioned into $S_1(2,4,2^{2m})$'s, each of which is 1-resolvable.

3.4.3 Remark: The construction of 3.4.2 is directly connected with the construction of packings of spreads in odd-dimensional projective spaces over $\text{GF}(2)$, cf. Barlotti [4], Beutelspacher [10].

Although the listing of these results may not be complete, it is natural to ask, for instance, if there exists a 2-resolvable $S_1(4,4,v)$ for some positive integer v . A little consideration of the parameters involved will give a hint as to how to proceed in this case.

3.4.4 Fact: Let v be a positive integer. If there exists a 2-resolvable $S_1(4,4,v)$, it is to be partitioned into $\binom{v-2}{2} S_1(2,4,v)$'s. A necessary condition for the existence is that $v \equiv 1,4 \pmod{12}$.

3.4.5 Heuristics: In order to construct a 2-resolution of an $S_1(4,4,v)$ it would be nice if the construction of $\binom{v-2}{2} S_1(2,4,v)$'s could be reduced to a single one, which under the action of a group generates the whole 2-resolution.

In accordance with the preceding sections it is reasonable to require $v-2$ to be a prime, such that the $\binom{v-2}{2}$ necessary transformations are given by the affine transformations

$$\pi_{\lambda,g} : x \mapsto \lambda x + g,$$

where $g \in \text{GF}(p)$ and $\lambda \in \Lambda$, Λ being a system of representatives of the cosets of $\text{GF}(p)^* \pmod{\langle 1, -1 \rangle}$. Thus one has to consider primes

$p \equiv 2, 11 \pmod{12}$ and the corresponding set $X = \text{GF}(p) \cup \{\infty, \infty'\}$, where

$\{\infty, \infty'\}$ is a set of two symbols, fixed by each $\pi_{\lambda,g}$, and disjoint

from $\text{GF}(p)$. The problem is to construct an $S_1(2,4,p+2)(X, \mathcal{B})$, the block

set of which consists of a complete system of representatives of the

orbits of $\binom{X}{4}$ under $\{\pi_{\lambda,g} \mid \lambda \in \Lambda, g \in \text{GF}(p)\}$. The smallest prime p ,

for which these considerations may apply, is $p = 11$.

The following attempt to construct a 2-resolution of $S_1(4,4,13)$ leads

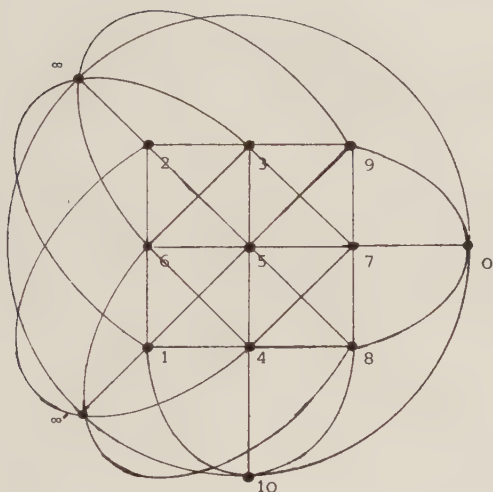
to a "near"-2-resolution the deficiency of which will be discussed afterwards. Nevertheless this seems to be the best approach to a 2-resolution.

By the considerations of 3.4.5 one therefore has to construct an $S_1(2,4,13)$ $(X, \mathcal{B})$ on the set $X = \text{GF}(11) \cup \{\infty, \infty'\}$, such that the class of blocks forms a complete system of representatives of the orbits of $\binom{X}{4}$ under the action of the group $T = \{\pi_{\lambda, g} \mid \lambda \in \text{GF}(p)^{*2}, g \in \text{GF}(p)\}$. Observe that T is a subgroup of $\text{PSL}(2,11)$ and that it acts sharply 2-homogeneously on $\text{GF}(11)$. It therefore seems to be reasonable to construct $\mathcal{B}$ as the class of orbits of certain subgroups of $\text{PGL}(2,11)$ - in accordance with the procedure which has been applied successfully in 3.1.

On the other hand, any $S_1(2,4,13)$ is isomorphic to $\text{PG}(2,3)$. Thus, if there are groups generating the blocks of $(X, \mathcal{B})$, they can be found in $\text{PGL}(3,3)$. Such a subgroup is given by the stabilizer of a line in $\text{PG}(2,3)$, which is isomorphic to $\mathcal{T}_4$. The subgroups $\mathcal{O}_4$ and $\mathcal{S}_4$ of $\text{PGL}(2,11)$ on the other hand are determined in Huppert:Endliche Gruppen, Berlin 1967. It follows that these subgroups of $\text{PGL}(2,11)$ do not act in a proper manner on the $S_1(2,4,13)$.

Yet the following construction shows that the above approach seems to be interesting.

3.4.6 Construction: Recalling 2.3.15 it is clear that the elements of $\text{GF}(11) \cup \{\infty, \infty'\}$ can be considered as the points of $S_1(2,4,13)$ in the following manner:



Here again, $GF(11)$ is canonically identified with the set $\{0\} \cup N_{10}$.

It remains to determine the orbits of the blocks

$$B_0 = \{\infty, \infty, 0, 10\}$$

$$B_1 = \{\infty, 1, 5, 9\}$$

$$B_2 = \{\infty, 2, 4, 7\}$$

$$B_3 = \{\infty, 3, 6, 8\}$$

$$B_4 = \{\infty, 1, 3, 7\}$$

$$B_5 = \{\infty, 4, 6, 9\}$$

$$B_6 = \{\infty, 2, 5, 8\}$$

$$B_7 = \{1, 2, 6, 10\}$$

$$B_8 = \{0, 2, 3, 9\}$$

$$B_9 = \{0, 5, 6, 7\}$$

$$B_{10} = \{3, 4, 5, 10\}$$

$$B_{11} = \{0, 4, 8, 1\}$$

$$B_{12} = \{7, 8, 9, 10\}$$

under the action of $T = \{ \pi_{\lambda, g} \mid \lambda \in \text{GF}(11)^{\times 2}, g \in \text{GF}(11) \}$ where

$$\pi_{\lambda, g}(x) := \lambda x + g \text{ for } x \in \text{GF}(11)$$

$$\pi_{\lambda, g}(\rho) = \rho \quad \text{if } \rho \in \{\infty, \infty'\}.$$

By methods of Beth [7] it is clear that the blocks $B_0, \dots, B_6$ generate different orbits of length $|T| = 5 \cdot 11$. Clearly $B_7, \dots, B_{12}$ also generate orbits of length $|T|$, since by the cardinalities the stabilizer of each B_i , $7 \leq i \leq 12$ has to be the identity $\{\pi_{1,0}\}$. Furthermore, it is easily checked that $B_7, \dots, B_{11}$ generate disjoint orbits $T(B_i)$, $7 \leq i \leq 11$, while the orbit $T(B_{12})$ of B_{12} is the same as that of B_{11} , ($B_{12} = \frac{1}{4} \cdot B_{11} + 7$). Thus it is proved that for $\beta = \{B_i \mid 0 \leq i \leq 12\}$ and $X = \text{GF}(11) \cup \{\infty, \infty'\}$ (X, β) is an $S_1(2, 4, 13)$ such that $(\pi)_{\pi \in T}$ is a family of subclasses of $\binom{X}{4}$ with the property that for each $\pi \in T$ there exists a unique $\pi' \in T$ such that $|\pi\beta \cap \pi'\beta| = 1$. In this sense the $\pi\beta$ are "almost" disjoint.

The construction 3.4.6 apparently is the first approach to generate a 2-resolution of an $S(4, 4, v)$. The parameter $v = 13$ is the smallest one for which an $S_1(2, 4, v)$ exists, but the approach of 3.4.6 does not seem to be successful in this case.

The outstanding problem to investigate 3-resolutions of $S(4, 4, v)$'s shall be treated in the following chapters.

CHAPTER 4: PARTITIONING ALL QUADRUPLES INTO STEINER QUADRUPLE SYSTEMS

4.1 Introduction

In analogy with the preceding sections the question arises as to what can be done to partition the system $\binom{X}{4}$ of all quadruples on a set X into Steiner Quadruple Systems on X .

As usual, one would like to start the investigation of this problem by considering some examples on small sets X for which one can expect rather uncomplicated solutions.

It has been proved by Hanani [29] that a Steiner Quadruple System on a finite set X exists if and only if $|X| \geq 4$ and

$$|X| \equiv 2 \text{ or } 4 \pmod{6}.$$

Therefore the smallest nontrivial case to consider is $|X| = 8$:

Although there exists a (unique) SQS(8), cf. 2.3.12, from the fact that the $S_1(3,3,7)$ is not 2-resolvable, cf. 3.2.1, it follows from 2.4.2 that $S_1(4,4,8)$ cannot be 3-resolvable.

This leads to the next case $|X| = 10$:

It was shown by Kramer and Mesner [34] that there is no partition of the system $S_1(4,4,10)$ of all quadruples of a 10-set into Steiner quadruple systems $S_1(3,4,10)$. Again with the help of a computer, Kramer and Mesner [35] derived the following negative result for the case $|X| = 14$: There is no 3-resolution of $S_1(4,4,14)$, which admits an automorphism of order 11.

Following Lindner and Rosa [36] this is all that presently is known

about the 3-resolvability of the systems $S_1(4,4,v)$.

For system with $|X| \geq 14$ practically nothing in general is known at the moment, but under extra hypotheses some information can be obtained on the resolvability of $(X, \binom{X}{t})$.

Let $v \equiv 2, 4 \pmod 6$ be a positive integer, $v \geq 4$. Let X be a set of order v .

If $\binom{X}{4}$ is 3-resolvable the $\binom{v}{4} = \frac{v(v-1)(v-2)(v-3)}{4 \cdot 3 \cdot 2 \cdot 1}$ 4-subsets of X can be partitioned into $v-3$ Steiner systems $S_1(3,4,v)$.

Taking over the idea suggested in [35] the further investigations will deal with such partitions of $\binom{X}{4}$ into Steiner systems $S_1(3,4,v)$ which admit an automorphism of order $v-3$, where $v-3$ is a prime.

Without loss of generality it then can be assumed that in these cases $X = G \cup \{\alpha, \beta, \gamma\}$, where α, β, γ are three distinct symbols disjoint from G , G being a cyclic group of order $v-3$, that acts on itself by translation leaving α, β, γ fixed. Furthermore it can be assumed that

$G = \mathbb{Z}_{v-3}$. Since this restriction even in the case $v = 14$ made extensive computer search necessary [35], it is conceivable to require some more properties of the systems $S_1(3,4,v)$, which partition $\binom{X}{4}$.

Because each of these SQS(v) (X, β_i) , $i \in \mathbb{N}_{v-3}$, will contain a block $\{\alpha, \beta, \gamma, x_i\}$ with $x_i \in G$, G acts transitively on the systems of the partition and it is reasonable to consider the partition as $\{\beta_g \mid g \in G\}$ where for each $g \in G$ $\beta_g = \beta_0 + g$ and (X, β_0) is a SQS(v).

In order to construct such a partition one has to define a suitable initial system (X, β_0) . While in [35] for the case $v = 14$ the existence of such an initial system could be excluded by computer, for the general study of this already restricted type of partitions it is necessary

to impose some more conditions upon the system (X, β_0) .

In this situation, recalling the idea of Schreiber [45] and Wilson [54] it is a most natural generalization to define (X, β_0) in a similar manner. This will be done in the next section, where for technical reasons more general - even infinite - abelian groups are considered.

4.2 Definition and Necessary Conditions

In this section the Schreiber-Wilson 2-resolution-method of complete 3-designs (cf. 3.2.3) shall be generalized to Steiner Quadruple Systems and complete 4-designs.

4.2.1 Definition: Let G be an abelian group such that $6 \in \text{Aut } G$.

Let α, β, γ be three distinct symbols which are not contained in G .

Let $X = G \cup \{\alpha, \beta, \gamma\}$ and $\binom{X}{4}$ be the set of all 4-subsets of X .

A partition $\{\beta_g \mid g \in G\}$ of $\binom{X}{4}$ with the following properties,

$$(i) \quad \{Q \in \binom{G}{4} \mid \sum_{q \in Q} q = 0\} \subset \beta_0$$

$$(ii) \quad \forall g \in G \quad \beta_g = \beta_0 + g$$

$$(iii) \quad \forall g \in G \quad (X, \beta_g) \text{ is a Steiner Quadruple System,}$$

is called a stratified-weight-3-resolution over G and will be referred to as an SW_3 -resolution.

4.2.2 Remark: If G is a finite abelian group, then $6 \in \text{Aut } G$ iff

$|G| \equiv 1, 5 \pmod{6}$, which is equivalent with $|X| = 2, 4 \pmod{6}$ and $|X| \geq 4$,

the necessary and sufficient conditions for the existence of an

$S_1(3, 4, |X|)$.

4.2.2 Agreement: Throughout this section G and X are as in 4.2.1.

If in the following the term SW_3 -resolution is used without further specifications, it is an SW_3 -resolution over G fulfilling the properties of 4.2.1.

The following observations describe the blocks of the "initial" system (X, β_0) as far as their portion of G , i.e. their intersection with G , is concerned.

4.2.3 Lemma: Let $\{\beta_g \mid g \in G\}$ be an SW_3 -resolution and $Q \in \beta_0 \cap \binom{G}{4}$.

Then
$$\sum_{q \in Q} q = 0.$$

Proof: Let $Q = \{x, y, z, u\}$. Then there is an element $h \in G$ such that $x+y+z+u = 4h$.

From 4.2.1 it follows that

$$Q-h = \{x-h, y-h, z-h, u-h\} \in \beta_0,$$

hence $Q \in \beta_h = \beta_0 + h$. Since $\{\beta_g \mid g \in G\}$ is assumed to be a partition of $\binom{X}{4}$ this is only possible if $h = 0$. $\#$

Since (X, β_0) ought to be a Steiner Quadruple System each 3-subset of X has to determine a unique block of size 4 in which it is contained.

The blocks $Q \in \beta_0 \cap \binom{G}{4}$ only contain those 3-subsets $\{x, y, z\}$ of G such that $u = -(x+y+z)$ is not an element of $\{x, y, z\}$.

The 3-subsets $\{x, y, z\}$ with $u \in \{x, y, z\}$ therefore have to be treated separately:

4.2.4 Definition: a) Let $T \in \binom{G}{3}$ such that $-\sum_{t \in T} t \in T$. Then T is called

a degenerate 3-subset of G .

b) For an SW_3 -resolution $\{\beta_g \mid g \in G\}$ a block $Q \in \beta_0$ is said to be of type i, if $|Q \cap \{\alpha, \beta, \gamma\}| = i$, where $i \in \{0, 1, 2, 3\}$.

4.2.5 Lemma: Let $Q \in \mathcal{B}_0$ in an SW_3 -resolution. Then Q is of type 1 iff q contains a degenerate 3-subset.

Proof: " $\Rightarrow$ " : Let $Q \cap G = \{x, y, z\}$. If

$$u := -(x+y+z) \notin \{x, y, z\}$$

then $\{x, y, z, u\} \in \mathcal{B}_0 \cap \binom{G}{4}$. But because $(X, \mathcal{B}_0)$ is an SQS the 3-subset $\{x, y, z\}$ can only occur in Q .

" $\Leftarrow$ " : Let $T \in \binom{G}{3}$ be degenerate and contained in $Q \in \mathcal{B}_0$. If $Q \setminus T$ were contained in G , then $\sum_{q \in Q} q \neq 0$. By 4.2.3 this is not possible. $\#$

From the preceding lemmata it is clear that every $T \in \binom{G}{3}$ is contained in a block of type 0 or type 1. Furthermore all those 3-subsets S of X are covered, which are of the form

$$S = \{x, y, \rho\}, \text{ where } \{x, y\} \in \binom{G}{2}, \rho \in \{\alpha, \beta, \gamma\}$$

and there exists an element z such that $\{x, y, z\}$ is degenerate.

These subsets S shall be considered more closely:

4.2.6 Proposition: Let $P \in \binom{G}{2}$. Then either one of the following holds:

- (i) There are exactly three distinct degenerate 3-subsets of G which contain P .
- (ii) There is exactly one degenerate 3-subset of G containing P .

Proof: Let $P = \{x, y\}$. Then the only degenerate 3-subsets of G which contain P are of the form $\{x, y, z_i\}$, $i \in \mathbb{N}_3$, where

$$z_1 := -2x - y, \quad z_2 := -x - 2y, \quad z_3 := -\frac{x+y}{2}.$$

The following cases are to be considered:

a) The elements z_1, z_2, z_3 of G are all distinct and disjoint from P .

Then obviously the sets $\{x, y, z_i\}$, $i \in \mathbb{N}_3$, are three distinct degenerate 3-subsets of G which contain P .

b) The elements z_1, z_2, z_3 are not all distinct. Several subcases are to be distinguished:

b⁽¹⁾) $z_1 = z_2$ implies $x = y$ which is impossible.

b⁽²⁾) $z_1 = z_3$ implies $x = -\frac{x+y}{2} = -2x-y$.

b⁽³⁾) $z_2 = z_3$ implies $y = -\frac{x+y}{2} = -2y-x$.

b⁽²⁾) says that there is only one degenerate 3-subset of G containing P , namely $\{x, y, z_2\}$, since $z_2 = x$ or $z_2 = y$ would imply $z_1 = z_2 = z_3$. Accordingly b⁽³⁾) shows that $\{x, y, z_1\}$ is the only degenerate 3-subset which contains P .

c) The elements z_1, z_2, z_3 are not all disjoint from P . Then there are several possibilities:

c⁽¹⁾) $z_1 = x$ is equivalent to b⁽²⁾.

c⁽²⁾) $z_1 = y$ implies $x = -y$.

c⁽³⁾) $z_2 = x$ is equivalent to c⁽²⁾.

c⁽⁴⁾) $z_2 = y$ is equivalent to b⁽³⁾.

c⁽⁵⁾) $z_3 = x$ is equivalent to c⁽¹⁾.

c⁽⁶⁾) $z_3 = y$ is equivalent to c⁽⁴⁾.

In the case c⁽²⁾) the only degenerate 3-subset containing the set

$P = \{x, y\}$ is the set $\{x, y, z_3\} = \{x, -x, 0\}$. $\#$

4.2.7 Definition: A 2-subset of G fulfilling condition (ii) of 4.2.6 is called doubly-degenerate.

4.2.8 Lemma: (i) If Q is a block of type 2 in an SW_3 -resolution then $Q \cap G$ is a doubly degenerate 2-subset of G .

(ii) If P is a doubly degenerate 2-subset then in an SW_3 -resolution there is a unique block of type 2 containing P ,

Proof: (i) Let $Q = \{x, y, \rho, \tau\}$ be a block of type 2, where $\{x, y\} \in \binom{G}{2}$, $\{\rho, \tau\} \in \binom{\{\alpha, \beta, \gamma\}}{2}$. Let $\{\sigma\} = \{\alpha, \beta, \gamma\} \setminus \{\rho, \tau\}$. Then there is a unique block R containing $\{x, y, \sigma\}$, say $R = \{x, y, \sigma, t\}$. Since (X, β_0) is a SQS, t cannot be in $\{\alpha, \beta, \gamma\}$. Hence R is of type 1 and $\{x, y, t\}$ is a degenerate 3-subset by 4.2.5. Since $\{x, y, \rho\}$ and $\{x, y, \tau\}$ occur already in a block of (X, β_0) there cannot be another block of type 1 containing $\{x, y\}$. Hence $\{x, y\}$ is a doubly degenerate 2-subset.

(ii) follows immediately from 4.2.7 and 4.2.6.

#

The following observation will completely classify all doubly degenerate 2-subsets of G :

4.2.9 Lemma: Let $P \in \binom{G}{2}$. P is doubly-degenerate iff one of the following holds:

- (i) $P = \{x, -3x\}$ for some $x \in G \setminus \{0\}$
- (ii) $P = \{x, -x\}$ for some $x \in G \setminus \{0\}$.

Proof: If $P = \{x, y\}$ is doubly-degenerate then either $b^{(2)}$ or $b^{(3)}$ or $c^{(2)}$ of the proof of 4.2.6 holds. $b^{(2)}$ and $b^{(3)}$ imply (i), while

$c^{(2)}$ implies (ii).

Conversely, it is obvious that there is only one degenerate 3-subset which contains P . $\#$

Summarizing these results it is immediate that the blocks of type 0,1,2 cover all 3-subsets S of X , unless $S \in \left\{ \begin{smallmatrix} \alpha, \beta, \gamma, 0 \\ 3 \end{smallmatrix} \right\}$. Hence the only block of type 3 is the 4-set $\{\alpha, \beta, \gamma, 0\}$.

The following proposition will draw a first conclusion of the above analysis of blocks of type 1.

4.2.10 Proposition: Let H be a subgroup of G with $6 \in \text{Aut } H$. If there exists a SW_3 -resolution of $\begin{pmatrix} X \\ 4 \end{pmatrix}$ then there exists a SW_3 -resolution of $\begin{pmatrix} Y \\ 4 \end{pmatrix}$ where $Y = H \cup \{\alpha, \beta, \gamma\}$.

Proof: For $h \in H$ let $\mathcal{Q}_h$ be the following system: $\mathcal{Q}_h = \mathcal{Q}_0 + h$ where

$$\mathcal{Q}_0 = \{Q \in \begin{pmatrix} Y \\ 4 \end{pmatrix} \mid Q \in \mathcal{B}_0\}.$$

Then for $h \in H$ the $\mathcal{Q}_h$ are disjoint systems in $\begin{pmatrix} Y \\ 4 \end{pmatrix}$ since

$$\mathcal{Q}_h = \{Q \in \begin{pmatrix} Y \\ 4 \end{pmatrix} \mid Q \in \mathcal{B}_h\} \text{ and for } h \in H \text{ the } \mathcal{B}_h \text{ are disjoint.}$$

On the other hand, if $Q \in \begin{pmatrix} Y \\ 4 \end{pmatrix}$, then there is a unique $h \in G$ such that

$Q \in \mathcal{B}_h$. Hence $Q' := Q - h \in \mathcal{B}_0$, where the following cases are possible:

$$\text{a) } Q' \text{ is of type 0: Then } 0 = \sum_{q' \in Q'} q' = \sum_{q \in Q} q - h \text{ which implies } \sum_{q \in Q} q = 4h.$$

Since $Q \subset \text{Hit}$ it follows that $h \in H$.

b) Q' is of type 1: Then $Q = T \cup \{\rho\}$ where $T - h$ is a degenerate 3-subset

of G and $\rho \in \{\alpha, \beta, \gamma\}$. Hence $-\sum_{s \in T-h} s = -\sum_{t \in T} (t-h) \in T-h$ which

implies $t' + \sum_{t \in T} t = 4h$ for some $t' \in T$ and hence $h \in H$.

c) Q' is of type 2: Then $Q = P \cup \{\rho, \tau\}$ where $P-h$ is a doubly degenerate 2-subset of G and $\{\rho, \tau\} \in \binom{\{\alpha, \beta, \gamma\}}{2}$. Then $P-h$ is equal to $\{x, -x\}$

or $\{x, -3x\}$ for some $x \in G \setminus \{0\}$. Since $P \subset H$ it follows that $h \in H$.

d) Q' is of type 0: Then $Q = \{\alpha, \beta, \gamma, h\}$ where $h \in H$.

Therefore $\{\mathcal{Q}_h \mid h \in H\}$ is a partition of $\binom{Y}{4}$.

It remains to show that $(Y, \mathcal{Q}_0)$ is a Steiner Quadruple System on Y :

Let T be a 3-subset of Y . Then there exists a unique block $B \in \mathcal{B}_0$ containing T . If $T \in \binom{H}{3}$ then clearly $B \in \mathcal{Q}_0$, since $-\sum_{t \in T} t \in H$.

The other cases are obvious by 4.2.9. #

The main purpose of the following sections is to derive necessary and sufficient conditions under which an initial system of an SW_3 -resolution may be constructed. Proposition 4.2.10 has shown that any SW_3 -resolution over G induces an SW_3 -resolution of H if H is a subgroup of G having $\sigma : x \mapsto 6x$ as an automorphism. If G is finite, from remark 4.2.2 it follows that $|G| \equiv 1, 5 \pmod{6}$ and hence one has $|H| \equiv 1, 5 \pmod{6}$ for any subgroup $H < G$, whence $6 \in \text{Aut } H$ is a consequence. Therefore it shall be assumed that G is of prime order.

If G is an infinite group with torsion, the torsion subgroups being subgroups can be treated like the finite groups above, while, if G is infinite torsionfree, without loss of generality it can be assumed that $\mathbb{Z} \subset G$.

It is immediate, that in this case a smallest infinite subgroup $H < G$ with $6 \in \text{Aut } H$ is a group isomorphic to the additive group of the ring $\mathbb{Z}[\frac{1}{6}]$. Without loss of generality the following conditions may be assumed.

4.2.11 Conditions: Henceforth it is assumed that $G = \mathbb{Z}_p$ for some prime $p \geq 5$ if G is finite or $G = \mathbb{Z}[\frac{1}{6}]$ if G is infinite; i.e., G is considered as the additive group of the field $\text{GF}(p)$ respectively of the ring $\mathbb{Z}[\frac{1}{6}]$.

4.2.12 Remark: In this situation it makes sense to talk about an element $1 \in G$.

It is clear that the condition $6 \in \text{Aut } G$ means nothing but that the elements 2 and 3 are units in $\text{GF}(p)$ respectively $\mathbb{Z}[\frac{1}{6}]$.

The investigations carried out above were concerned with the determination of the intersections of blocks of an initial SQS $(X, \mathcal{B}_0)$ with G .

In order to derive necessary and sufficient conditions for the existence of such a system $(X, \mathcal{B}_0)$ it remains to classify the intersections of blocks with $\{\alpha, \beta, \gamma\}$.

4.2.13 Definition: Let $\mathcal{D}^G$ be the set of doubly degenerate 2-subsets of G , $\mathcal{V}^G$ be the set of degenerate 3-subsets of G . Let $\Omega^G = (\mathcal{D}^G \cup \mathcal{V}^G, \mathcal{E}^G)$ be the graph on the vertex set $\mathcal{D}^G \cup \mathcal{V}^G$ where two vertices $R, R' \in \mathcal{D}^G \cup \mathcal{V}^G$ are joined by an edge $e \in \mathcal{E}^G$ iff one of the following holds:

- (i) $|R \cap R'| = \max\{|R|, |R'|\} - 1$
- (ii) $\exists g \in G \setminus \{0\} : R = R' + g$.

A mapping $c : \mathcal{D}^G \cup \mathcal{V}^G \rightarrow 2^{\{\alpha, \beta, \gamma\}}$ is called an admissible vertex colouring of Ω^G , if

- (i) $|c(R)| = 4 - |R|$ for each $R \in \mathcal{D}^G \cup \mathcal{V}^G$
- (ii) $c(R) \not\subseteq c(R')$ for each edge $\{R, R'\} \in \mathcal{E}^G$.

If there is no danger of confusion Ω^G will be denoted by Ω ; $\nabla^G, \mathcal{D}^G, \mathcal{E}^G$ by $\nabla, \mathcal{D}, \mathcal{E}$ respectively.

For $x \in G \setminus \{0\}$ let Ω_x be the connected component of Ω which contains the vertex $\{-x, x\}$.

4.2.14 Theorem: There exists an SW_3 -resolution over G iff there exists an admissible vertex colouring of Ω .

Proof: To prove necessity let $\{\beta_g \mid g \in G\}$ be an SW_3 -resolution. By 4.2.5 and 4.2.8 for each $R \in \mathcal{D} \cup \nabla$ there is a unique block $Q_R \in \beta_0$ such that $R = Q_R \cap G$. Then the mapping

$$c^{\beta_0} : \mathcal{D} \cup \nabla \longrightarrow 2^{\{\alpha, \beta, \gamma\}}$$

given by $c^{\beta_0}(R) = Q_R \cap \{\alpha, \beta, \gamma\}$

is an admissible colouring: Clearly one has $|c^{\beta_0}(R)| = 4 - |R|$ for each $R \in \mathcal{D} \cup \nabla$.

Let $R, R' \in \mathcal{D} \cup \nabla$ be joined by an edge $e \in \mathcal{E}$.

Then either $|R \cap R'| = \max\{|R|, |R'|\} - 1$

or $R = R' + g$ for some $g \in G \setminus \{0\}$.

In the first case by observing that (X, β_0) is an SQS one has

$|Q_R \cap Q_{R'}| \leq 2$, which implies

$$c^{\beta_0}(R) \cap c^{\beta_0}(R') \leq 3 - \max\{|R|, |R'|\}.$$

The fact that $2 \leq |R|, |R'| \leq 3$ immediately implies that $c^{\beta_0}(R) \neq c^{\beta_0}(R')$

In the second case, i.e. $R = R' + g$ for some $g \in G \setminus \{0\}$, $c^{\beta_0}(R) = c^{\beta_0}(R')$

would imply $Q_R \in \beta_0 \cap \beta_g$, which contradicts the assumption that

$\{\beta_g \mid g \in G\}$ is a partition of $\binom{X}{4}$.

The sufficiency will be shown as follows:

Let $c: \mathcal{D} \cup \mathcal{T} \rightarrow 2^{\{\alpha, \beta, \gamma\}}$ be admissible.

Then $\{\alpha, \beta, \gamma\} \not\subseteq \text{im } c$. Therefore define $\{\alpha, \beta, \gamma, 0\} \in \mathcal{B}$.

For each $R \in \mathcal{D} \cup \mathcal{T}$ let $Q_R := R \cup c(R) \in \mathcal{B}$.

Furthermore if $Q \in \binom{G}{4}$ such that $\sum_{q \in Q} q$ let $Q \in \mathcal{B}$.

Then $(X, \mathcal{B})$ is an SQS on X since one has the following properties

- a) For each $R \in \mathcal{D} \cup \mathcal{T}$ Q_R is a 4-subset of X .
- b) Each 3-subset of G is contained in a unique element of $\mathcal{B}$.
- c) By 4.2.6 (i) all 3-subsets S of X , where $S \cap G \in \binom{G}{2} \setminus \mathcal{D}$, are in a unique block in $\mathcal{B}$.
- d) If $D \in \mathcal{D}$ by 4.2.6 (ii) there is a unique element $T \in \mathcal{T}$ which contains D . By b) T is contained in a unique block B , say $B = T \cup \{\rho\}$, $\rho \in \{\alpha, \beta, \gamma\}$. Thus $D \cup \{\rho\}$ is covered uniquely by a block B , since by definition
- e) $c(D) = \{\tau, \sigma\}$ does not contain ρ . Therefore $D \cup \{\tau\}$ and $D \cup \{\sigma\}$ are in a unique block, too.

For each $g \in G$ define $\mathcal{B}_g := \mathcal{B} + g$.

If $Q \in \mathcal{B}_0 \cap \mathcal{B}_h$ for some $h \in G \setminus \{0\}$, then $Q = Q' + h$, where $Q' \in \mathcal{B}_0$.

By definition $Q, Q' \in \binom{G}{4}$, which for $S := Q \cap G$ and $S' := Q' \cap G$ implies $S, S' \in \mathcal{D}$ or $S, S' \in \mathcal{T}$. Since $S = S' + h$, by the assumption on c one has $c(S) \not\subseteq c(S')$. Therefore $Q \not\subseteq Q' + h$, which contradicts $Q \in \mathcal{B}_0 \cap \mathcal{B}_h$.

Thus $\{\mathcal{B}_g \mid g \in G\}$ is an SW_3 -resolution over G . $\#$

By this theorem it is clear that in order to construct SW_3 -resolutions one has to find admissible colourings of the graph Ω . The study of

this graph Ω can be simplified by the following lemma:

4.2.15 Lemma: Let $x \in G \setminus \{0\}$. Then the connected component Ω_x is isomorphic to Ω_1 .

Proof: Clearly for $x \in G \setminus \{0\}$ by the choice of G , cf. 4.2.11, the mapping defined by

$$g \mapsto x \cdot g \quad \text{for each } g \in G$$

is an injective homomorphism of Ω .

Hence $x\Omega_1 \subset \Omega_x$.

Now let $R \in \mathcal{D} \cup \mathcal{V}$ which is adjacent to some xR' where $R' \in \mathcal{D} \cup \mathcal{V}$.

Then by definition Ω either

$$|xR' \cap R| = \max\{|R|, |R'|\} - 1$$

or $xR' = R + g$ for some $g \in G \setminus \{0\}$.

In the first case observing that $xR' \cap R \subset xG$, and using the definition of $\mathcal{D}$ and $\mathcal{V}$, one has $R \subset xG$.

In the second case one has to observe that by 4.2.4 and 4.2.9 there are positive integers $(\lambda_r)_{r \in R}$ such that

$$\sum_{r \in R} \lambda_r = 4$$

and $\sum_{r \in R} \lambda_r r = 0$.

$xR' = R + g$ then implies

$$\sum_{r = xr' - g} \lambda_r (xr' - g) = 0$$

Hence $g \in xG$ and $R \subset xG$. $\#$

From this observation it follows that it is enough to study the properties of the component Ω_1 of Ω , in order to find out about the existence of admissible colourings. Necessary conditions for this shall be obtained by considering suitable subgraphs of Ω .

4.2.16 Definition: Let Γ be the subgraph of Ω , which is generated by the set of vertices $\mathcal{D}$. A mapping $c_\Gamma : \mathcal{D} \longrightarrow \left(\begin{smallmatrix} \alpha, \beta, \gamma \\ 2 \end{smallmatrix}\right)$ is called Γ -admissible, if it is a vertex colouring of Γ . For $x \in G \setminus \{0\}$ let Γ_x be the connected component of Γ which contains the vertex $\{x, -x\}$. For a Γ -admissible colouring c_Γ let $\{\rho, \tau\} := c_\Gamma(\{-x, x\})$. The x -characteristic transposition (of c_Γ) is the transposition $w_x = (\rho\tau)$ on $\{\alpha, \beta, \gamma\}$.

4.2.17 Theorem: Let $x \in G \setminus \{0\}$ and $A := \langle -1, -2, -3 \rangle^*$ be the group generated by $\{-1, -2, -3\}$ in $\text{Aut } G$. Let $c_\Gamma : \mathcal{D} \longrightarrow \left(\begin{smallmatrix} \alpha, \beta, \gamma \\ 2 \end{smallmatrix}\right)$ be Γ -admissible and w_x be the x -characteristic transposition of c_Γ . Then the following holds

(i) A is a group of automorphisms of Γ_x having two orbits on the vertex set of Γ_x .

(ii) For each vertex D of Γ_x and each $a \in \{-1, -3\}$ one has $c_\Gamma(aD) = w_x(c_\Gamma(D))$.

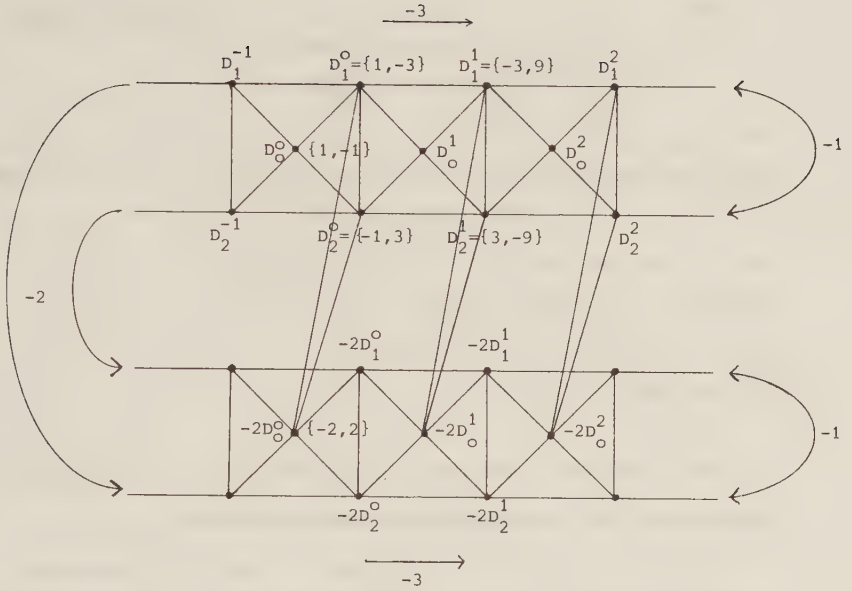
(iii) For each vertex D of Γ_x and $a = -2$ one has
 either $c_\Gamma(aD) = c_\Gamma(D)$
 or $c_\Gamma(aD) = w_x(c_\Gamma(D))$.

Proof: By Observation 4.2.15 it is sufficient to prove these statements for the component Γ_1 of Γ only.

Since $\{1, -1\}$ is a vertex of Γ_1 by definition 4.2.13 (i) the $\{1, -3\}$, $\{-1, 3\}$, $\{1, -\frac{1}{3}\}$, $\{-1, \frac{1}{3}\}$ are adjacent to $\{1, -1\}$ and therefore in Γ_1 . For $i \in \mathbb{Z}$ let $D_0^i := (-3)^i \{1, -1\}$, $D_1^i := (-3)^i \{1, -3\}$ and $D_2^i := (-3)^i \{-1, 3\}$. Then it is clear that for $\lambda \in \{1, 2\}$ D_λ^i is adjacent to both D_λ^{i-1} and D_λ^{i+1} for each $i \in \mathbb{Z}$. This in turn implies that for $\lambda \in \{1, 2\}$ and $i \in \mathbb{Z}$ D_λ^i is adjacent to D_0^i and D_0^{i+1} . By lemma 4.2.9 these are all the adjacencies which are induced by condition (i) of definition 4.2.13. It remains to find all the adjacencies due to condition (ii) of 4.2.13:

For $x \in G \setminus \{0\}$ let $D = \{x, -3x\}$. Let $g \in G \setminus \{0\}$ be such that $D+g \in \mathcal{D}$. Then either $g = x$ or $g = 2x$. While if for $z \in G \setminus \{0\}$ $D' = \{z, -z\}$ $h \in G \setminus \{0\}$ is such that $D'+h \in \mathcal{D}$, it follows that $h = \pm \frac{z}{2}$. This implies that for each $i \in \mathbb{Z}$ D_1^i and D_2^i are adjacent, since $\{1, -3\} + 2 = \{3, -1\}$. Furthermore, since $\{1, -3\} + 1 = \{2, -2\} = \{-1, 3\} - 1$, one has the adjacency of $-2D_0^i$ and both D_1^i and D_2^i for each $i \in \mathbb{Z}$. Iteration shows that the vertex set of Γ_1 is the set $\{aD_v \mid v=0,1, a \in \langle -1, -2, -3 \rangle^*\}$, while the edges are as described above.

A picture will show the graph locally:



From these considerations it is immediate that $\langle A \rangle^*$ is a group of automorphisms of Γ_1 . Thus (i) is proved.

Now (ii) and (iii) will be shown jointly. Without loss of generality one can assume that $c_\Gamma(\{1, -1\}) = \{\beta, \gamma\}$.

From the picture it is clear, that $D_1^0 = \{1, -3\}$ has to have one of the colours $\{\alpha, \beta\}$ or $\{\alpha, \gamma\}$. Again without loss of generality it is assumed that $c_\Gamma(D_1^0) = \{\alpha, \beta\}$. It then is immediate that $c_\Gamma(D_2^0) = \{\alpha, \gamma\}$, $c_\Gamma(D_1^1) = \{\beta, \gamma\}$, which implies $c_\Gamma(D_1^1) = \{\alpha, \gamma\} = w_1(c_\Gamma(D_1^0))$ and $c_\Gamma(D_2^1) = \{\alpha, \beta\} = w_1(c_\Gamma(D_2^0))$.

Iteration for all powers of -3 shows that for $\lambda \in \{1, 2\}$ and for $i \in \mathbb{Z}$

one has

$$c_{\Gamma}(D_{\lambda}^i) = \begin{cases} \{\alpha, \beta\} & \text{if } \lambda+i \equiv 1 \pmod{2} \\ \{\alpha, \gamma\} & \text{if } \lambda+i \equiv 0 \pmod{2} \end{cases}$$

and $c_{\Gamma}(D_0^i) = \{\beta, \gamma\}$.

From these considerations and the picture it is clear, that for each $i \in \mathbb{Z}$

$$c_{\Gamma}(-2D_0^i) = \{\beta, \gamma\}$$

which in turn implies that for $\lambda \in \{1, 2\}$

either $c_{\Gamma}(-2D_{\lambda}^i) = c_{\Gamma}(D_{\lambda}^i)$

or $c_{\Gamma}(-2D_{\lambda}^i) = w_1(c_{\Gamma}(D_{\lambda}^i))$.

Thus one has (ii) and (iii). #

In order to demonstrate the use of the graph Γ and the implications of theorem 4.2.17 the following examples shall be considered.

4.2.18 Example: From section 4.1 it is known that there is no 3-resolution of $\binom{X}{4}$ into Steiner Quadruple Systems if the set X has cardinality 8 or 10.

Hence there is no SW_3 -resolution over $\mathbb{Z}_5$ respectively $\mathbb{Z}_7$.

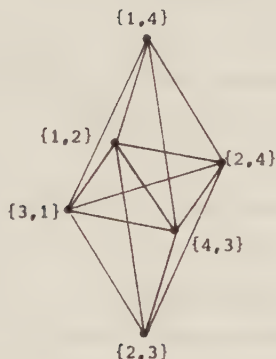
Therefore the above classifications must lead to a contradiction in these cases.

a) Let $G = \mathbb{Z}_5$. Certainly $6 \in \text{Aut } \mathbb{Z}_5$, since $x \mapsto 6x = x \pmod{5}$. Suppose there is a SW_3 -resolution over $\mathbb{Z}_5$ with the initial system $\mathcal{B}_0$.

Then $\{\alpha, \beta, \gamma, 0\} \in \mathcal{B}_0$.

The doubly degenerate 2-subsets of $\mathbb{Z}_5$ are the sets $\{1, 4\}$, $\{2, 3\}$ and $\{1, 2\}$, $\{2, 4\}$, $\{4, 3\}$, $\{3, 1\}$.

Hence Γ has the form



which immediately implies that Γ is not 3-colourable. In spite of this contradiction it is easy to construct one $S_1(3,4,8)$ on the set $X := \mathbb{Z}_5 \cup \{\alpha, \beta, \gamma\}$ with a system of blocks whose intersections with G are zero-sum-quadruples, degenerate triples and doubly degenerate pairs. To be able to do so the edges $\{1,2\} \bullet \bullet \bullet \{4,3\}$ and $\{2,4\} \bullet \bullet \bullet \{3,1\}$ must be removed from Γ , since these had been there by condition 4.2.13(ii), which was due to the requirement that all systems $\mathcal{B}_g$ of the resolution should be G -translates of the initial system $\mathcal{B}_0$. The graph Γ' without these edges being an octahedron is easily 3-colourable:

The double-degenerate 2-subsets of $\mathbb{Z}_5$ therefore determine the following blocks:

$$\{1,4,\beta,\gamma\}, \{2,3,\beta,\gamma\}$$

$$\{1,2,\alpha,\beta\}, \{4,3,\alpha,\beta\}$$

$$\{2,4,\alpha,\gamma\}, \{3,1,\alpha,\gamma\}.$$

From this the degenerate 3-subsets have to be distributed as follows:

$$\{0,1,4,\alpha\} , \{0,2,3,\alpha\}$$

$$\{0,1,3,\beta\} , \{0,2,4,\beta\}$$

$$\{0,1,2,\gamma\} , \{0,3,4,\gamma\} .$$

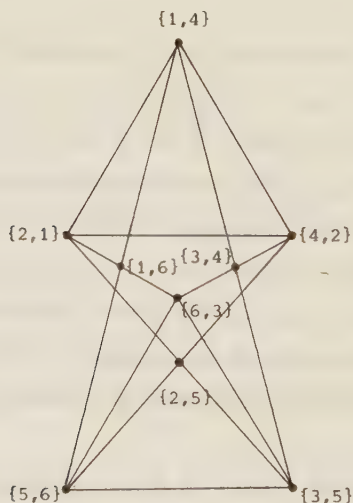
The only zero-sum-quadruple in $\mathbb{Z}_5$ is the set

$$\{1,2,3,4\} .$$

With a total of fourteen blocks this is an $S_1(3,4,8)$.

b) Let $G = \mathbb{Z}_7$. Trivially $6 \in \mathbb{Z}_7^*$.

The existence of an SW_3 -resolution would lead to a graph Γ which again only after the removal of the edges due to 3.2.13 (ii) becomes a 3-colourable graph Γ' :



Let $\{\alpha,\beta,\gamma,0\}$ be a block. Due to a colouring of Γ' the doubly-degenerate 2-subsets of $\mathbb{Z}_7$ are distributed as follows:

$\{1,4,\alpha,\beta\}$	$\{2,5,\alpha,\beta\}$	$\{6,3,\alpha,\beta\}$
$\{4,2,\beta,\gamma\}$	$\{1,6,\beta,\gamma\}$	$\{3,5,\beta,\gamma\}$
$\{2,1,\alpha,\gamma\}$	$\{3,4,\alpha,\gamma\}$	$\{5,6,\alpha,\gamma\}$

This induces a distribution of the degenerate 3-subsets of $\mathbb{Z}_7$:

$\{2,6,4,\alpha\}$	$\{4,5,1,\beta\}$	$\{1,3,2,\gamma\}$
$\{1,0,5,\gamma\}$	$\{2,0,3,\alpha\}$	$\{4,0,6,\beta\}$
$\{0,1,6,\alpha\}$	$\{0,2,5,\beta\}$	$\{0,4,3,\gamma\}$
$\{6,2,0,\gamma\}$	$\{5,4,0,\alpha\}$	$\{3,1,0,\beta\}$
$\{5,3,1,\alpha\}$	$\{3,6,2,\beta\}$	$\{6,5,4,\gamma\}$

Together with the 5 zero-sum quadruples of $\mathbb{Z}_7$ these 25 blocks above form an $S_1(3,4,10)$. #

These two examples show that condition (ii) of 4.2.13, which corresponds to (ii) in 4.2.1, induces an essential part of the restrictions which are imposed on an initial system.

The following corollary shall reduce some of these restrictions to properties of G .

4.2.19 Corollary: If there exists a Γ -admissible vertex colouring of Γ ,

where G is finite and hence $G = \mathbb{Z}_p$ for some prime $p \geq 5$, then

$$\text{ord}_p(-3) \equiv 2 \pmod{4}.$$

Proof: Apply the corresponding step of the proof of 3.2.3 to the subgraph C_{-3} of Γ , which is generated by the vertices $\{(-3)^i, (-3)^{i+1}\} \pmod{p}$ for $i \in \mathbb{Z}$. #

If G is infinite there is no similar conclusion, since C_{-3} then is a 2-way-path-graph which trivially can be 2-coloured.

Corollary 4.4.16 being a necessary condition for the existence of an SW_3 -resolution is not sufficient: -3 is a primitive element of $GF(11)$, hence $\text{ord}_{11}(-3) = 10$.

But as mentioned in section 4.1 there is no 3-resolution of $S_1(4,4,14)$ admitting an automorphism of order 11. Therefore there is no SW_3 -resolution over $\mathbb{Z}_{11}$, either. Hence more necessary conditions have to be derived. Reconsidering theorem 4.2.17, it is clear that (iii) is a rather unsatisfactory description of the action of the automorphism -2 : Applying powers of -2 , it is not clear that this implies the same power of the permutation on the set $\{\alpha, \beta, \gamma\}$. In the sequel this deficiency will be removed.

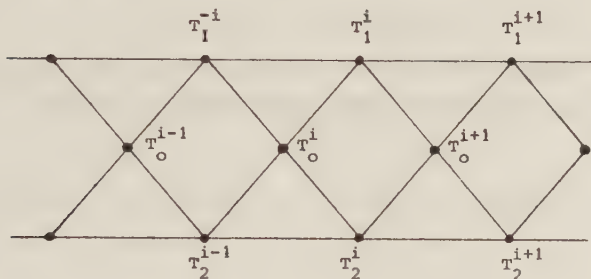
For this purpose one has to consider the class of degenerate 3-subsets, according to an earlier remark. In order to do so the necessary definitions and notations are introduced:

4.2.20 Definition: Let Δ be the subgraph of Ω which is generated by the set $\mathbb{T}$ of vertices.

A mapping $c_\Delta : \mathbb{T} \rightarrow \{\alpha, \beta, \gamma\}$ is called Δ -admissible if it is a vertex colouring of Δ . For $x \in G \setminus \{0\}$ let Δ_x be the connected component of Δ which contains the vertex $\{-x, 0, x\}$.

4.2.21 Remark: By 4.2.15 it is clear that for each $x \in G \setminus \{0\}$ the graph Δ_x is isomorphic to Δ_1 , whence it is sufficient to study the properties of Δ_1 only.

4.2.22 Notation and Observation: Δ_1 contains the following subgraph N



which is the subgraph in Δ_1 generated by the vertices $\{T_\lambda^i\}_{i \in \mathbb{Z}; \lambda=0,1,2}$ where for $i \in \mathbb{Z}$ and $\lambda \in \{0,1,2\}$

$$T_\lambda^i := (-2)^i T_\lambda$$

and

$$T_\lambda := \begin{cases} \{-1, 0, 1\} & \text{if } \lambda = 0 \\ \{-2, 0, 1\} & \text{if } \lambda = 1 \\ \{-1, 0, 2\} & \text{if } \lambda = 2 \end{cases}.$$

Hence $-2 \in \text{Aut } G$ is an automorphism of Δ_1 . Therefore, in order to determine the vertices connected with this subgraph N it is sufficient to do this for the vertices T_0^i , T_1^i and T_2^i for some $i \in \mathbb{Z}$.

Furthermore let C_{-2} denote the subgraph of Δ_1 , which is generated by the set of vertices $\{T_\lambda^i \mid \lambda \in \{1,2\}, i \in \mathbb{Z}\}$.

The following study of special subgraphs of Δ_1 requires a computation of the degenerate 3-subsets of G , which are vertices of these subgraphs.

In order to avoid the problem that if $G = \mathbb{Z}_p$ is finite vertices with different parameters could be identified mod p , one has to observe the following:

By the above examples and remarks it can be assumed that $p > 11$.

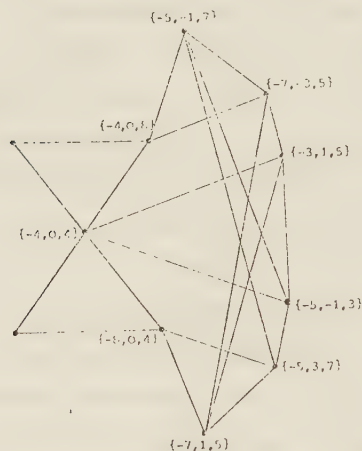
Since only admissible colourings shall be studied and - cf. 4.2.15 -

$$\text{ord}_{17}(-3) \equiv 0 \pmod{4}$$

$$\text{ord}_{19}(-3) = 9 \equiv 1 \pmod{4},$$

one has $p = 13$ or $p \geq 23$.

This justifies the "parametrization" of the following subgraph M of Δ_1 :



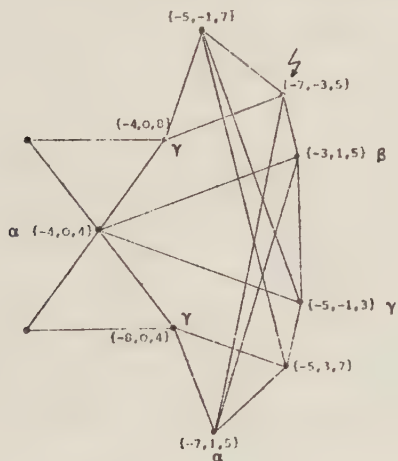
The subgraph M in Δ_1 .

It is clear that the listed 3-subsets of G are degenerate and hence they are vertices of Δ_1 . The drawn edges are due to an intersection being a 2-subset of G (cf. 4.2.13 (i)) or to the fact that one vertex is a G -translate of another vertex (c.f. 4.2.13 (ii)).

From this one can deduce the first important fact that will be helpful in the following

4.2.23 Observation: If there exists an Δ -admissible colouring c of Δ then $c(\{-8,0,4\}) \neq c(\{-4,0,8\})$.

Proof: Considering M without loss of generality one has, if $c(\{-8,0,4\}) = c(\{-4,0,8\})$,



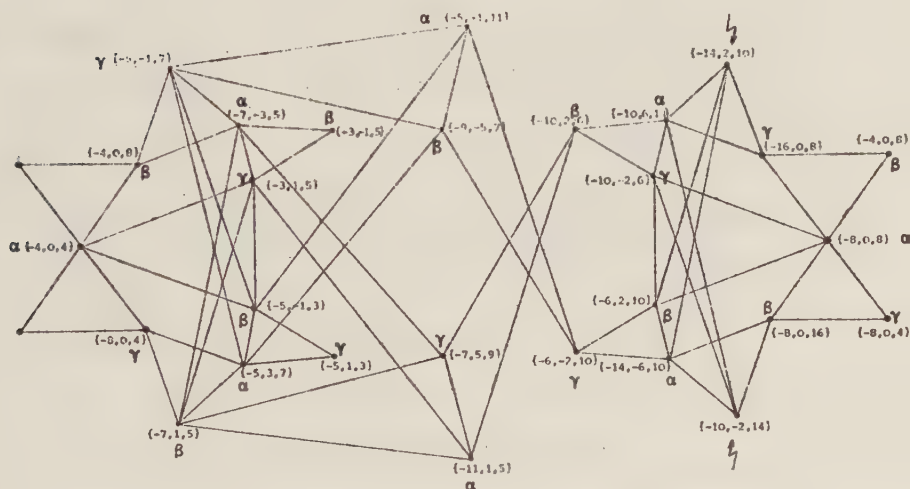
for instance, the impossibility to colour $\{-7,-3,5\}$, if one takes into consideration that $\{-4,0,4\}$, $\{-5,-1,3\}$ and $\{-3,1,5\}$ have to be coloured with the three different colours α, β, γ . #

From this subgraph the most important property of Δ -admissible colourings can be deduced.

4.2.26 Lemma: If there exists an Δ -admissible colouring c of Δ then

$$c(\{-4,0,8\}) = c(\{-3,1,5\}) .$$

Proof: Suppose $c(\{-4,0,8\}) \neq c(\{-3,1,5\})$. Without loss of generality this enforces the following distribution of colours (cf. 4.2.24) on L .

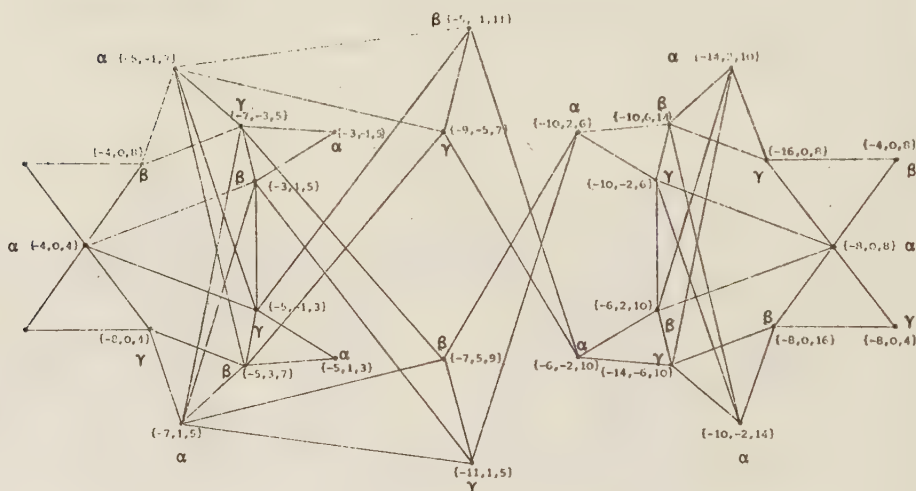


From 4.2.23 it follows that $c(\{-4,0,4\}) = \{\alpha\}$ and w.l.o.g. $c(\{-4,0,8\}) = \{\beta\}$ and $c(\{-8,0,4\}) = \{\gamma\}$.

Thus $c(\{-3,1,5\}) = \{\gamma\}$ and $c(\{-5,-1,3\}) = \{\beta\}$. It is easy to derive the colours of all other vertices of L - except the vertices $\{-14,2,10\}$

and $\{-10, -2, 14\}$ which are connected to three vertices having three different colours. This is a contradiction. $\#$

4.2.27 Corollary: The restriction of an Δ -admissible colouring to the subgraph L is - up to a permutation of $\{\alpha, \beta, \gamma\}$ - uniquely determined as follows:



Admissible colouring of L (unique mod $\gamma_{\{\alpha, \beta, \gamma\}}$)

The properties of admissible colourings which have been deduced above, shall be summarized in the following theorem.

4.2.28 Theorem: The following are equivalent:

- (i) There exists an SW_3 -resolution over G .
- (ii) There exists an admissible colouring of Ω .
- (iii) There exists an Δ -admissible colouring of Δ and an Γ -admissible colouring c_Γ of Γ such that for each $D \in \mathcal{D}$ $c_\Gamma(-2D) = w_x(c_\Gamma(D))$ where w_x is the x -characteristic transposition of c_Γ .
- (iv) There exists an Δ -admissible colouring of Δ and, if $G = \mathbb{Z}_p$ for some prime p

$$\text{ord}_p(-3) \equiv 2(4) .$$

Proof: Clearly (i) $\iff$ (ii) is only a repetition of 4.2.14. The other equivalence shall be proved by (ii) $\implies$ (iv) $\implies$ (iii) $\implies$ (ii).

(ii) $\implies$ (iv) is clear by observing that for an admissible colouring c of Ω the restrictions $c|_{\mathcal{D}}$ and $c|_{\Gamma}$ are Γ - (resp. Δ -) admissible. To prove (iv) $\implies$ (iii) it is sufficient to show that there exists a colouring $c : \Gamma_1 \rightarrow \binom{\{\alpha, \beta, \gamma\}}{2}$ of Γ_1 such that $c(\{1, -1\}) = \{\beta, \gamma\}$ and $c(-2D) = (\beta\gamma)c(D)$ for each $D \in \mathcal{D}$.

By 4.2.17 this is equivalent to the existence of a mapping

$$\bar{c} : \mathcal{D} \rightarrow \{\{\alpha, \beta\}, \{\alpha, \gamma\}\} \text{ such that } \bar{c}(\rho D) \neq \bar{c}(D) \text{ for each } D \in \mathcal{D} \text{ and each } \rho \in \{-1, -2, -3\} \text{ where } \mathcal{D} := \{a\{1, -3\} \mid a \in \{-1, -2, -3\}^*\}.$$

By the facts mentioned in the proof of 4.2.19 such a mapping $\bar{c}$ exists iff for $\rho \in \{-1, -2, -3\}$ the order of the subgroups $\langle \rho \rangle^* \triangleleft \text{Aut } G$ is infinite or a number congruent 2 mod 4. For $G = \mathbb{Z}[\frac{1}{6}]$ this is always true. If $G = \mathbb{Z}_p$ for some prime $p > 5$ this is true iff

$\text{ord}_p(-3) \equiv \text{ord}_p(-2) \equiv 2 \pmod{4}$. Both properties are guaranteed by (iv), cf. 4.2.24 (iii).

To prove (iii) $\implies$ (ii) one only has to show that the colourings of Γ and Δ can be "synchronized" to an admissible colouring of Ω .

It is enough to show this for the component Ω_1 .

Clearly Γ_1 is a subgraph of Ω_1 . Therefore the connected components of Δ being subgraphs of Ω_1 are the components $(-3)^i \Delta_1$ for $i \in \mathbb{Z}$.

Hence Γ_1 is the only Γ -component being in Ω_1 . By (iii) there is a colouring c_Γ of Γ_1 as follows:

$$c_\Gamma(\{1, -1\}) = \{\beta, \gamma\}$$

$$c_\Gamma(\{1, -3\}) = \{\alpha, \gamma\}$$

$$c_\Gamma(aD) = (\beta\gamma)c(D)$$

for each vertex D of Γ_1 and each $a \in \{-1, -2, 3\} \subset \text{Aut } G$.

Again by (iii) and 4.2.27 there is a colouring c_Δ of Δ_1 such that for $a \in \{-1, -2\} \subset \text{Aut } G$

$$c_\Delta(a\{1, 0, -1\}) = \{\alpha\}$$

$$c_\Delta(a\{1, -3, 5\}) = (\beta\gamma)\{\beta\}.$$

Clearly c_Δ can be extended to the other components $(-3)^i \Delta_1$ by putting

$$c_\Delta \Big|_{(-3)^i \Delta_1} = c_\Delta \Big|_{\Delta_1} \circ (\beta\gamma)^i.$$

Then $c := c_\Delta \cup c_\Gamma$ is an admissible colouring of Ω . #

4.2.29 Conclusion: In order to construct an SW_3 -resolution over G it

is sufficient to construct Δ -admissible colourings, if $G = \mathbb{Z}[\frac{1}{6}]$

or $G = \mathbb{Z}_p$ for some prime $p > 5$ such that $\text{ord}_p(-3) \equiv 2 \pmod{4}$ and

$\text{ord}_p(-2) \equiv 2 \pmod{4}$.

By the quadratic reciprocity law it follows that a prime p of the form $p \equiv 23 \pmod{24}$ fulfils these two conditions.

4.2.30 Example: From earlier remarks it follows that the smallest prime p for which $\text{ord}_p(-3) \equiv \text{ord}_p(-2) \equiv 2 \pmod{4}$ is $p = 23$. Recalling 4.2.27 it is clear that for a Δ -admissible colouring c_Δ one can assume

$$\text{that} \quad \{-1, 0, 2\} \xrightarrow{c_\Gamma} \{\beta\}$$

$$\text{and} \quad \{-3, -1, 5\} \longrightarrow \{\alpha\}.$$

$$\text{Hence} \quad \{-3, -1, 2\} \longrightarrow \{\gamma\}$$

$$\text{which implies} \quad \{-8, 4, 12\} \longrightarrow \{\beta\}.$$

$$\text{Since} \quad \{-8, 0, 4\} \longrightarrow \{\gamma\}$$

$$\text{one has} \quad \{-8, 2, 4\} \longrightarrow \{\alpha\}.$$

From the third line it then follows that

$$\{-3, 2, 4\} \longrightarrow \{\beta\}.$$

$$\text{Since also} \quad \{-3, 1, 5\} \longrightarrow \{\beta\}$$

$$\text{one has} \quad \{-12, 4, 20\} \longrightarrow \{\beta\} \text{ too. But in}$$

$$\mathbb{Z}_{23} \text{ this means} \quad \{-3, 4, 11\} \longrightarrow \{\beta\}, \text{ which is a}$$

$$\text{contradiction to} \quad \{-3, 2, 4\} \longrightarrow \{\beta\}.$$

Hence there is no Δ -admissible colouring over $G = \mathbb{Z}_{23}$. Thus the conditions $\text{ord}_p(-2) \equiv 2 \pmod{4}$ and $\text{ord}_p(-3) \equiv 2(4)$ are not sufficient for the existence of an SW_3 -resolution.

4.2.31 Remark: Methods similar to those of the example 4.2.30 can be applied to the primes $p = 47$ and $p = 71$ with a negative result, too. This leads to the conclusion that possibly a condition quite different from the two cited above has to be fulfilled in order to guarantee the existence of an SW_3 -resolution. In the remaining sections of this chapter the investigations leading to a classification of those groups G admitting an SW_3 -resolution will be carried out.

4.3. A Lifting Theorem.

The purpose of this section is to show that if there exists an SW_3 -resolution over $G = \mathbb{Z}_p$ for some prime $p > 5$ it can be "lifted" to an SW_3 -resolution over $\mathbb{Z}[\frac{1}{6}]$.

4.3.1 Agreement: The conditions and notations of 4.2 shall be assumed for this section too.

4.3.2 Lemma: Let $G = \mathbb{Z}[\frac{1}{6}]$ and R be a vertex in the connected component Ω_1 of Ω . If $R \subset xG$ then $x \in \langle -1, -2, -3 \rangle^*$.

Proof: By 4.2.17 and a remark in the last step of the proof 4.2.28 one only has to show that for $R \in \Delta_1$ $R \subset xG$ implies $x \in \langle -1, -2 \rangle^*$. The statement is certainly true for vertices of the subgraph L , cf. 4.2.25. Let R be a vertex of Δ_1 . It then is connected to the subgraph L by a path of finite length. Two vertices - i.e. degenerate 3-subsets of G - are adjacent iff $|R' \cap R''| = 2$ or $R' = R'' + g$ for some $g \in G \setminus \{0\}$. Repeating the proof of 4.2.15 one has that $R' \subset xG$ implies $R'' \subset xG$. $\#$

4.3.3 Theorem: Let p be a prime such that $\text{ord}_p(-3) \equiv 2(4)$ and $\text{ord}_p(-2) \equiv 2(4)$. Let $\Omega^p := \Omega^{\mathbb{Z}_p}$ and $\Omega := \Omega^{\mathbb{Z}[\frac{1}{6}]}$. Let ϕ_p be the canonical epimorphism $\phi_p : \mathbb{Z}[\frac{1}{6}] \twoheadrightarrow \mathbb{Z}_p$ and $\overline{\phi}_p$ its extension to the power set of $\mathbb{Z}[\frac{1}{6}]$. If there is an admissible colouring c_p of Ω^p then there is an admissible colouring c of Ω such that for each vertex R of Ω

$$c(R) \subseteq c_p \circ \overline{\phi}_p(R).$$

Proof: Let Ω^* be the subgraph of Ω which consists of all vertices R of Ω such that $R \notin pG$, where $G := \mathbb{Z}[\frac{1}{6}]$.

By 4.2.15 and 4.3.2 this is the subgraph Ω^* generated by all vertices xR where R is a vertex in Ω_1 and $x \in G \setminus pG = \mathbb{Z}[\frac{1}{6}] \setminus p\mathbb{Z}[\frac{1}{6}]$.

Then $\{p^i \Omega^* \mid i \in \mathbb{N}\}$ is a partition of Ω into subgraphs isomorphic to Ω^* . For $i, j \in \mathbb{N}_0$, $i \neq j$, $p^i \Omega^*$ and $p^j \Omega^*$ are not connected. Hence it is sufficient to construct the required admissible mapping c only on the vertex set of Ω^* .

Let $\Omega^* = (\mathcal{D}^* \cup \mathcal{T}^*, \varepsilon^*)$ where $\mathcal{D}^* \subset \mathbb{Z}[\frac{1}{6}]$, $\mathcal{T}^* \subset \mathbb{Z}[\frac{1}{6}]$. Let $\Omega^p := \Omega^{\mathbb{Z}_p} = (\mathcal{D}_p \cup \mathcal{T}_p, \varepsilon_p)$ where $\mathcal{D}_p = \mathcal{D}^{\mathbb{Z}_p}$, $\mathcal{T}_p = \mathcal{T}^{\mathbb{Z}_p}$. Since p is fixed within the proof let ϕ denote $\overline{\phi}_p$.

Construct $c : \mathcal{D}^* \cup \mathcal{T}^* \rightarrow 2^{\{\alpha, \beta, \gamma\}}$ as follows: For $R \in \mathcal{D}^* \cup \mathcal{T}^*$ such that $\{\phi(R)\} = |R|$ define $c(R) = c_p(\phi(R))$. For $R \in \mathcal{T}^*$ such that $\phi(R) \in \mathcal{D}_p$ there are two possibilities:

Either $\phi(R) = \{a, -3a\}$ and $c_p\{a, -3a\} = \begin{cases} \{\alpha, \gamma\} \\ \{\alpha, \beta\} \end{cases}$ or $\phi(R) = \{2a, -2a\}$ and $c_p\{2a, -2a\} = \{\beta, \gamma\}$ for some $a \in \mathbb{Z}_p \setminus \{0\}$.

Then $R \in \mathbb{Z}[\frac{1}{6}]$ has either form (cf. 4.2.6)

$$R = \begin{cases} \{a+xp, a+yp, -3a-2xp-yp\} \\ \{2a+xp, 2a+yp, -2\frac{x+y}{2}p\} \end{cases} \quad \text{or}$$

where a is interpreted as the unique element $\phi^{-1}(a) \in \mathbb{Z}$, $1 \leq \phi^{-1}(a) \leq p-1$.

Then define

$$c(R) := \begin{cases} \begin{cases} \alpha & \text{if } x < y \\ \gamma & \text{if } x > y \end{cases} & \text{if } c_p(\phi(R)) = \{\alpha, \gamma\} \\ \begin{cases} \beta & \text{if } x < y \\ \alpha & \text{if } x > y \end{cases} & \text{if } c_p(\phi(R)) = \{\alpha, \beta\} \\ \begin{cases} \beta & \text{if } c_p(\phi(R)-a) = \{\alpha, \gamma\} \\ \gamma & \text{if } c_p(\phi(R)-a) = \{\alpha, \beta\} \end{cases} & \text{and } c_p(\phi(R)) = \{\beta, \gamma\} \end{cases}$$

It remains to show that c is admissible.

Case 1: $R, R' \in \mathcal{T}^*$ and $|R \cap R'| = 2$

a) $\phi(R), \phi(R') \in \mathcal{T}_p$ and $|\phi(R) \cap \phi(R')| = 2$: There is nothing to prove.

b) $\phi(R), \phi(R') \in \mathcal{T}_p$ and $|\phi(R) \cap \phi(R')| = 3$: Cannot exist.

c) $\phi(R) \in \mathcal{T}_p, \phi(R') \in \mathcal{D}_p$ $|\phi(R) \cap \phi(R')| = 2$. Then, since c_p is admissible, by construction $c(R) \cap c(R') = \emptyset$.

d) $\phi(R) \in \mathcal{D}_p, \phi(R') \in \mathcal{D}_p$ $|\phi(R) \cap \phi(R')| = 2$ and $\phi(R) = \phi(R') = \{a, -3a\}$.

Then for R and R' one has (1) or (2):

1) $R = \{a+xp, a+yp, -3a-2xp-yp\}$ and $R' = \{a+xp, a+yp, -3a-xp-2yp\}$.

Since $R, R' \in \mathcal{T}^*$ it follows that $x \neq y$ and one is smaller than the other.

2) $R = \{a-2yp-zp, a+yp, -3a+zp\}$ and $R' = \{a - \frac{y+z}{2}p, a+yp, -3a+zp\}$.

Since again $|R| = |R'| = 3$ one has $y > -\frac{x+z}{2}$, $-2y-z$ or $y < -\frac{x+y}{2}$, $-2y-2$.

Thus in both cases $c(R) \neq c(R')$ by construction.

e) $\phi(R) \in \mathcal{D}_p, \phi(R') \in \mathcal{D}_p$, $|\phi(R) \cap \phi(R')| = 2$ and $\phi(R) = \phi(R') = \{b, -b\}$.

Then one has $R = \{b+xp, -b+yp, -b-2xp-yp\}$.

$R' \in \mathcal{T}^*$ with $|R \cap R'| = 2$ can only have the form

$R' = \{b-xp-2yp, b+xp, -b+yp\}$ or $R' = \{b+3xp+2yp, b+xp, -b-2xp-yp\}$

which again by construction implies $c(R) \neq c(R')$.

f) $\phi(R) \in \mathcal{D}_p, \phi(R') \in \mathcal{D}_p$, $|\phi(R) \cap \phi(R')| = 1$. Then w.l.o.g. one has

$\phi(R) = \{a, -3a\}$ and $\phi(R') = \{a, -a\}$, which implies that R and R' have

the form $R = \{a+xp, a+yp, -3a-2xp-yp\}$, $R' = \{a+xp, a+yp, -a - \frac{x+y}{2}p\}$.

Since $\{a, -a\} - \frac{a}{2} = \{\frac{a}{2}, -\frac{3a}{2}\}$ and $c_p(\{a, -3a\}) = c_p(\{\frac{a}{2}, -\frac{3a}{2}\})$

by 4.2.28 one has $c(R) \neq c(R')$ by construction.

Case 2: $R \in \mathcal{V}^*$, $R' \in \mathcal{D}^*$ and $|R' \cap R| = 2$.

$$a) \phi(R) \in \mathcal{V}_p \quad \phi(R') \in \mathcal{D}_p.$$

Here nothing is to be proved.

$$b) \phi(R) \in \mathcal{D}_p \quad \phi(R') \in \mathcal{D}_p$$

cannot exist.

Case 3: $R, R' \in \mathcal{D}^*$, $|R \cap R'| = 1$.

Then $\phi(R)$, $\phi(R') \in \mathcal{D}_p$.

Case 4: $R, R' \in \mathcal{V}^*$, $R = R' + g$ for some $g \in \mathbb{Z}[\frac{1}{6}] \setminus \{0\}$.

a) $\phi(R)$, $\phi(R') \in \mathcal{V}_p$. Then one has $\phi(R) = \phi(R') + g_p$ where $g \equiv g_p \pmod{p}$.

Suppose $g_p \equiv 0 \pmod{p}$. Then if $R' = \{r, s, t\}$ w.l.o.g. one would have

$$2r + s + t = 0$$

and $r + 2s + t + 4xp = 0$ for some $x \in \mathbb{Z}[\frac{1}{6}] \setminus \{0\}$

which implies $r = s + 4xp$

and $r \equiv s \pmod{p}$.

This is a contradiction to $\phi(R)$, $\phi(R') \in \mathcal{V}_p$.

Hence $c(R) = c_p(\phi(R)) \not\equiv c_p(\phi(R')) = c(R')$.

$$b) \phi(R), \phi(R') \in \mathcal{D}_p.$$

Let $\phi(R') = \{a, -3a\}$. Then R' has the form $R' = \{a + 4xp, a + 4yp, -3a - 8xp - 4yp\}$.

Hence $R = R' + g$ has the form (1) or (2):

$$(1) R = \{a + 5xp - yp, a + xp + 3yp, -3a - 7xp - 5yp\} \text{ where } g = (x - y)p.$$

Since R' and R are 3-subsets one either has

$$4x < 4y \text{ and } 5x - y < x + 3y$$

$$\text{or} \quad 4y < 4x \text{ and } x + 3y < 5x - y.$$

Therefore $c(R) \not\equiv c(R')$.

(2) $R = \{2a+7xp+yp, 2a+3xp+5yp, -2a-5xp-3yp\}$ where $g = a+3xp+yp$.

Then by construction $c(R) \neq c(R')$.

Case 5: $R, R' \in \hat{\mathcal{D}}^*$, $R = R' + g$ for some $g \in \mathbb{Z}[\frac{1}{6}] \setminus \{0\}$.

Then $\phi(R), \phi(R') \in \mathcal{D}_p$ and $\phi(R) = \phi(R') + g_p$ where $g \equiv g_p \pmod{p}$.

If $g_p \equiv 0 \pmod{p}$ then $R, R' \subset p \mathbb{Z}[\frac{1}{6}]$.

Hence $c(R) \neq c(R')$. $\#$

From this theorem it is clear that every admissible colouring c_p of $\Omega \mathbb{Z}_p$ for some prime p is a factor in an admissible colouring c of $\Omega \mathbb{Z}[\frac{1}{6}]$ such that

$$\begin{array}{ccc} \Omega \mathbb{Z}[\frac{1}{6}] & & \\ \phi \downarrow \text{mod } p & \searrow & 2\{\alpha, \beta, \gamma\} \\ \Omega \mathbb{Z}_p & \nearrow & \end{array}$$

$$c \subseteq c_p \circ \phi.$$

In this sense the class of admissible colourings of $\Omega \mathbb{Z}[\frac{1}{6}]$ is "universal".

Therefore the next section will be devoted to the study of this class of colourings.

4.4 Admissible Colourings over $\mathbb{Z}[\frac{1}{6}]$

4.4.1 Definition: Let $\Omega = \Omega^{\mathbb{Z}[\frac{1}{6}]} = (\mathcal{D} \cup \mathcal{T}, \mathcal{E})$ where $\mathcal{D}$ is the set of doubly-degenerate 2-subsets of $\mathbb{Z}[\frac{1}{6}]$, $\mathcal{T}$ the set of degenerate 3-subsets of $\mathbb{Z}[\frac{1}{6}]$ and $\mathcal{E} := \mathcal{E}^{\mathbb{Z}[\frac{1}{6}]}$. Let

$c : \mathcal{D} \cup \mathcal{T} \rightarrow 2^{\{\alpha, \beta, \gamma\}}$ be given as follows: For $D \in \mathcal{D}$ let

$$c(D) := \begin{cases} \{\alpha, \gamma\} & \text{if } \sum_{d \in D} d < 0 \\ \{\beta, \gamma\} & \text{if } \sum_{d \in D} d = 0 \\ \{\alpha, \beta\} & \text{if } \sum_{d \in D} d > 0 \end{cases}$$

For $R \in \mathcal{T}$, $R = \{x, y, z\}$ where $x < y < z$ let

$$c(R) = \begin{cases} \{\beta\} & \text{if } 2x+y+z = 0 \\ \{\alpha\} & \text{if } x+2y+z = 0 \\ \{\gamma\} & \text{if } x+y+2z = 0 \end{cases}$$

This mapping is called the standard labelling of $(\Omega^{\mathbb{Z}[\frac{1}{6}]})$.

4.4.2 Theorem: The standard labelling is an admissible colouring of $\Omega^{\mathbb{Z}[\frac{1}{6}]}$.

Proof: In chapter 5 one can find this theorem as special case of a more general theorem. To illustrate the derivation of this later theorem a proof will be given here.

Let $c : \mathcal{D} \cup \mathcal{T} \rightarrow 2^{\{\alpha, \beta, \gamma\}}$ be the standard labelling.

Clearly $c|_{\mathcal{D}}$ is Γ -admissible, cf. 4.2.28.

Let $T \in \mathcal{T}$ and $D \in \mathcal{D}$ such that

$$|T \cap D| = 2.$$

Then for some $x \in \mathbb{Z}[\frac{1}{6}] \setminus 0$

either $T = \{x, -3x, 5x\}$ and $D = \{x, -3x\}$

or $T = \{-x, 0, x\}$ and $D = \{x, -x\}$.

In both cases one has $c(T) \cap c(D) = \emptyset$ by construction.

To show the Δ -admissibility of $c|_{\overline{V}}$ let $R, R' \in \overline{V}$.

Case 1: $|R \cap R'| = 2$.

Then $R = \{x, y, z\}$ and $R' = \{x, y, u\}$, where by 4.2.6 u and z are two distinct elements of

$$K := \{-2x-y, -2y-x, -\frac{x+y}{2}\}.$$

Up to symmetry one of the following cases holds:

$$(1) \begin{cases} x < y < -2x - y \\ x < y < -2y - x \\ x < y < -\frac{x+y}{2} \end{cases} \quad \begin{matrix} \text{and} \\ \text{and} \\ \text{and} \end{matrix}$$

$$(2) \begin{cases} x < y < -2x - y \\ x < -2y - x < y \\ x < -\frac{x+y}{2} < y \end{cases} \quad \begin{matrix} \text{and} \\ \text{and} \\ \text{and} \end{matrix}$$

$$(3) \begin{cases} x < -2x - y < y \\ x < -2y - x < y \\ x < -\frac{x+y}{2} < y \end{cases} \quad \begin{matrix} \text{and} \\ \text{and} \\ \text{and} \end{matrix}$$

In each of these cases it is clear that $c(R) \not\subseteq c(R')$.

Case 2: $R = R' + g$ for some $g \in \mathbb{Z}[\frac{1}{6}] \setminus \{0\}$.

Let $R = \{r_1, r_2, r_3\}$ $r_1 < r_2 < r_3$.

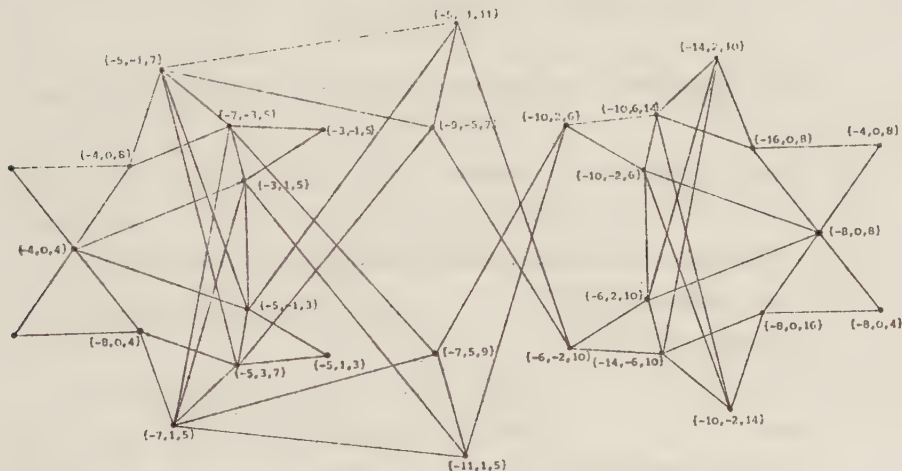
Then $R' = \{r'_1, r'_2, r'_3\}$ where $r'_i + g = r_i$ for $i \in \{1, 2, 3\}$.

If for some $i \in \{1, 2, 3\}$

$$r'_i + \sum_{r' \in R'} r' = 0 = r_i + \sum_{r \in R} r$$

then $g = 0$, which is a contradiction. $\#$

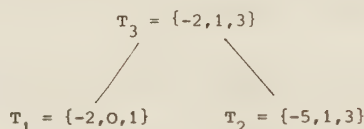
Recalling 4.2.27 the restriction of the standard labelling to the subgraph L is exactly the colouring given there



The restriction of the standard labelling to L .

This is not surprising since in 4.2.27 it has been shown that this colouring is unique mod $\mathcal{T}_{\{\alpha, \beta, \gamma\}}$. Surprising is the fact that the colouring is extendable to Δ_1 in a unique way.

4.4.3 Example: To determine the colour of the vertex $\{-2, 1, 3\}$ one has to observe that in Δ_1 one has



since T_1, T_2 being vertices of L they are already coloured $c(T_1) = \{\gamma\}$ $c(T_2) = \{\alpha\}$. This implies $c(T_3) = \{\beta\}$.

This example shows the technique of determining the colour of a vertex.

The set T_3 determines the sequence

$$d(T_3) = (1 - (-2), 3 - 1) = (3, 2)$$

of consecutive differences, which is well defined by the natural order related in $\mathbb{Z}[\frac{1}{6}]$.

Accordingly one has

$$d(T_1) = (2, 1)$$

and

$$d(T_2) = (6, 2).$$

Since multiplication by 2 does not change the colour of a vertex of L , for the above conclusion it would have been enough to know the colour of $d(\frac{1}{2} \cdot T_2) = (3, 1)$.

In this sense T_1 and T_2 have been coloured "earlier" than T_3 , i.e. for a suitable rank function defined on the set of vertices the ranks of T_1 and T_2 are smaller than the rank of T_3 .

Since this argument could as well have been carried out for $-T_3$, $-T_2$ and $-T_1$ it is not reasonable in general to consider the ordered sequence of pairwise differences.

The presentation of this example gives a hint that the colour of a vertex of Δ in an admissible colouring can be determined, i.e. determined uniquely. More exactly, this will be stated in the following

4.4.4 Theorem: Let c' be an admissible colouring of Ω , c be the standard labelling. For each connected component Ω_x of Ω there exists a permutation $\pi_x \in \mathcal{V}_{\{\alpha, \beta, \gamma\}}$ such that

$$c'|_{\Omega_x} = \pi_x \circ c|_{\Omega_x}.$$

Proof: By 4.2.17 and 4.2.28 it is sufficient to show this theorem only for $c'|_{\Delta_1}$.

Let $\mathcal{V}_1$ be the set of vertices of Δ_1 .

Recalling from 4.3.2 that if for two vertices $R, R' \in \mathcal{V}_1$.

$R = xR'$ holds for some $x \in \mathbb{Z}[\frac{1}{6}] \setminus \{0\}$ one has $x \in \langle -1, -2 \rangle^*$, it is possible to define a rank function

$$\text{rk} : \mathcal{V}_1 \longrightarrow \mathbb{N}$$

by the following procedure:

Let $R \in \mathcal{V}_1$, where $R = \{x, y, z\}$ and $x < y < z$.

Let $i \in \mathbb{Z}$ be chosen such that

$$2^i \{y-x, z-y\} \subset \mathbb{Z}$$

but not

$$2^i \{y-x, z-y\} \subset 2\mathbb{Z}.$$

Then let $\text{rk}(R) := 2^i(z-x) - 1$.

Before starting the essential part of the proof, some helpful remarks about the function rk shall be made:

1) Fact: $\text{rk} : \mathbb{T}_1 \rightarrow \mathbb{N}$ is surjective.

Because: Let $n \in \mathbb{N}$, then there is a pair a, b of positive integers such that $\text{gcd}(a, b) = 1$ and $a + b = n + 1$. Then

$$\text{rk}(-3a-2b, a-2b, a+2b) = a+b-1 = n.$$

2) Fact: Let $R \in \mathbb{T}_1$ such that $\text{rk}(R) \leq 2$. Then up to permutation of α, β, γ for any admissible colouring c' one has

$$c'(R) = c(R)$$

where c is the standard labelling.

This follows from the remarks after 4.4.2.

3) Technical definition: Let $R \in \mathbb{T}_1$, where

$$R = \{x, y, z\} \text{ and } x < y < z.$$

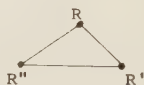
$$R \text{ is called of type } \begin{cases} \text{I if } 2x+y+z = 0 \\ \text{II if } x+2y+z = 0 \\ \text{III if } x+y+2z = 0. \end{cases}$$

The pair $\delta(R) = (y-x, z-y)$ is called the balance of R .

4) Fact: Let $R \in \mathbb{T}_1$. Then there are $R', R'' \in \mathbb{T}_1$ such that

$$\delta(R) = \delta(R') = \delta(R''),$$

types of R, R' and R'' are all distinct and R, R', R'' are mutually adjacent in Δ_1 :



Because: Without loss of generality R is of type I .

$$R = \{4x, 4y, 4z\} , \quad x < y < z , \quad z = -2x - y .$$

Then $R' = \{5x - y, x + 3y, -7x - 5y\} = R + (x - y)$ is of type II and adjacent (cf. 4.2.13) to R .

Analogously $R'' = \{7x + y, 3x + 5y, -5x - 3y\}$ is of type III and adjacent to both R and R' .

Now the theorem will be proved by induction on $\text{rk}(R)$:

For $\text{rk}(R) = 1$ (and $\text{rk}(R) = 2$) the theorem is true by Fact 2. Furthermore, one can assume that for these cases $c'(R) = c(R)$.

Let $n \in \mathbb{N}$ be a positive integer.

Assume the theorem is true for all $R \in \mathbb{V}_1$ such that $\text{rk}(R) \leq n$,

$$\text{i.e. } c'(R) = \begin{cases} \alpha & \text{if } R \text{ of type II} \\ \beta & \text{if } R \text{ of type I} \\ \gamma & \text{if } R \text{ of type III} . \end{cases}$$

Then let $R \in \mathbb{V}_1$ be of rank $n+1$.

If R is of type II then it will be sufficient to determine the colour of R' and R'' whose existence is guaranteed by Fact 4 , such that

$$\delta(R') = \delta(R'') = \delta(R) \text{ and } R' \text{ and } R'' \text{ are of type I (respectively type III).}$$

Furthermore it is sufficient to determine the colour of the vertex R'' of type III since $-R'$ is of type III and by induction hypothesis multiplication by -1 only interchanges β and γ .

Thus let R be of type III . Without loss of generality one can assume $R \subset \mathbb{Z}^3$ but not $R \subset 2\mathbb{Z}^3$. Let $R = \{x, y, z\}$ and $x < y < z$. The balance

$$\delta(R) = (y - x, z - y)$$

has the property

$$\gcd(y - x, z - y) \in \{1, 2, 4\} ,$$

since $4x = 3(x-y) + 2(y-z)$ and $R \in \mathbb{V}_1$ and $R \subset \mathbb{Z}$ but not $R \subset 2\mathbb{Z}$.

Hence $n+1 = \text{rk}(R) = 2^{-i}(z-x)$ where

$$2^i = \gcd(y-x, z-y) \text{ and } i \in \{0, 1, 2\}.$$

Then for $2^{-i}\delta(R)$ there are the following possibilities, where

$$(a, b) = 2^{-i}(y-x, z-y).$$

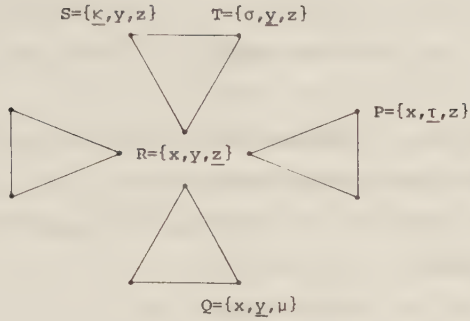
- A) Both a and b are odd, $a < b$
- B) Both a and b are odd, $a > b$
- C) a is even, b is odd, $a < b$
- D) a is even, b is odd, $a > b$
- E) a is odd, b is even, $a > b$
- F) a is odd, b is even, $a < b$.

Before carrying out the induction step for each of these cases some of the adjacencies of the vertex $R = \{x, y, z\}$ shall be considered more closely:

5) Notation: For the sake of clarity the following notation is used:

The underlined element $\underline{t}$ in a degenerate 3-subset $s = \{r, s, \underline{t}\}$ denotes that $r+s+2t = 0$.

6) Picture: The vertex $R = \{x, y, \underline{z}\}$ lies in the following subgraph of Δ_1 , the picture of which shows all the adjacencies that are used later:



7) Fact: Since $x < y < \underline{z}$ one has

- (i) $x < \underline{y} < \mu$ and $z < \mu$
- (ii) Either $\underline{\kappa} < y < z$ and $\sigma < \underline{y} < z$
 or $y < \underline{\kappa} < z$ and $\underline{y} < \sigma < z$
- (iii) $\sigma < y \iff y - x > z - y$
- (iv) $x < \kappa$ and $x < \sigma$.

Because: (i) $\mu \leq z$ would imply $x + 2y + \mu < 0$.

(ii) Since the standard labelling is an Δ -admissible colouring and R is of type III, S and T must be of type II and I respectively I and II.

(iii) $z - y < y - x = y - (-2z - y) = 2y + 2z$

iff

$$\sigma = -2y - z < y.$$

(iv) Analogous to (i).

By the help of these considerations one can proceed to the induction step.

Case A: If a and b are odd and $a < b$

then $A') \text{ rk}(T) \leq n$

and $A'') \text{ rk}(S) \leq n$.

In order to show $A')$ one has to recall that

$$a < b \iff y-x < z-y \iff y < \sigma.$$

Hence T has the form $\{y, \sigma, z\}$ where $y < \sigma < z$. Recalling that

$2^i b = z-y$ where $i \in \{0, 1, 2\}$ one has

$$\begin{aligned} z-\sigma &= z - (-2y-z) = 2z+2y \\ &= 2(z-y) + 4y \\ &\equiv 0 \pmod{2^i} \\ \sigma-y &= (-2y-z)-y = -4y + (y-z) \equiv 0 \pmod{2^i}. \end{aligned}$$

Hence $\text{rk}(T) \leq b \leq n$.

Proving $A'')$ one has $y < \kappa < z$.

$$\text{Then } z-\kappa = z - \left(-\frac{y+z}{2}\right) = 2z + \frac{y-z}{2}$$

$$\text{and } \kappa-y = -\frac{y+z}{2} - y = -2y + \frac{y-z}{2}.$$

Observing that from $R \subset \mathbb{Z}$ and a, b odd, it follows that $x = -3a-2b$

(cf. fact 1) one has $y-z \equiv 4 \pmod{8}$ and y, z odd.

This implies $z-\kappa \equiv \kappa-y \equiv 4 \pmod{8}$ and hence $z-\kappa \equiv 0 \pmod{2^i}$ and

$\kappa-y \equiv 0 \pmod{2^i}$. Thus $\text{rk}(S) = b \leq n$.

Since T is of type I and S is of type II one has that $c'(R) = \{\gamma\}$.

Case B: Recalling that in this case x, y, z must be odd and $2^i = 4$,

i.e. $y-x \equiv 4 \pmod{8}$ and $z-y \equiv 4 \pmod{8}$ one has from fact 7 (iv)

$$y-x > y-\sigma \text{ and } y-x > y-\kappa.$$

Furthermore it is obvious that

$$y-\sigma \equiv 0 \pmod{4}$$

$$y-\kappa \equiv 0 \pmod{4}.$$

Thus $\text{rk}(S) \leq n$ and $\text{rk}(T) \leq n$.

Since T is of type II and S is of type I it follows that $c'(R) = \{\gamma\}$.

Case C: In this case it will be shown that $\text{rk}(T) \leq n$ and $\text{rk}(Q) \leq n$.

Since $a < b$ the first assertion and its proof correspond to A' .

It remains to determine the rank of Q :

$$Q = \{x, y, \mu\} \text{ and } x < y < \mu.$$

$$\text{Since } \mu - y = (-2y - x) - y = -(x + y) - 2y = 2(z - y)$$

$$\text{one has } \text{rk}(Q) = \frac{a}{2} + b - 1 < a + b - 1 = \text{rk}(R) \leq n + 1.$$

Since T is of type I and Q is of type II by induction hypothesis one has $c'(R) = \{\gamma\}$.

Case D: Although one cannot find two different vertices which are of lower rank, of different type, and adjacent to R , a more detailed investigation will establish the induction step in this case too:

Since $a > b$ by fact 7 (iii) one has for

$$S = \{\kappa, y, z\} \text{ and } T = \{\sigma, y, z\}$$

$$\kappa < y < z \text{ and } \sigma < y < z.$$

It is easy to see that $\text{rk}(T) \leq n$:

$$y - \sigma < y - \kappa$$

$$\text{and } y - \sigma = 4y + (z - y).$$

Since a is even, b is odd, one has $\gcd(y - \kappa, z - y) = \gcd(y - \sigma, z - y)$ and $\text{rk}(T) \leq n$.

Furthermore it is easy to observe that

$$\text{rk}(S) = \text{rk}(R).$$

For $y-\kappa = 2y + \frac{z-y}{2}$ there are two cases to be considered:

(i) $\kappa \in \mathbb{Z}$. This is only possible if $z-y \equiv 0 \pmod{2}$. Since b is odd, a even, it follows that $y-x \equiv 0 \pmod{4}$.

Furthermore $z-y \equiv 0 \pmod{4}$ is impossible since this would imply $y-x \equiv 0(8)$, which by the argument used in fact 1 would lead to $R \subset 2\mathbb{Z}$.

Thus $z-y \equiv 2 \pmod{4}$, $\frac{z-y}{2} \equiv 1 \pmod{2}$

and hence $y-\kappa \equiv 1 \pmod{2}$.

Thus $\gcd(y-\kappa, z-y) = 1$ and

$$\text{rk}(S) = z-\kappa = \frac{3z+y}{2}.$$

Observing that in this case

$$\text{rk}(R) = \frac{1}{2}(z-x) = \frac{1}{2}(z-(-2z-y)) = \frac{3z+y}{2}$$

one has $\text{rk}(S) = \text{rk}(R) = n+1$.

(ii) $\kappa \in \frac{1}{2}\mathbb{Z}$. This is only possible if

$$z-y \equiv 1 \pmod{2}.$$

In this case $y-x = a$ and $z-y = b$.

Furthermore one has $\text{rk}(S) = 2z-2\kappa = 3z+y$.

Since $\text{rk}(R) = a+b = z-x = 3z+y$, the assertion $\text{rk}(S) = \text{rk}(R)$ follows.

It is now clear that $\text{rk}(S) = \text{rk}(-S)$ and $-S$ is of type III

$$-S = \{-z, -y, -\kappa\}.$$

Choose $i \in \mathbb{Z}$ such that the pair $(a', b') := 2^{-i} \delta(-S) = 2^i(z-y, y-\kappa)$,

called the reduced balance, is in $\mathbb{Z} \times \mathbb{Z}$ but not in $(2\mathbb{Z}) \times (2\mathbb{Z})$.

Then in either case (i) or (ii) one has

a' is even, b' is odd

and $a'+b' = \text{rk}(-S) = \text{rk}(S) = \text{rk}(R) = n+1$.

Again there are two cases to be considered:

(i') If $a' < b'$ this reduces to the case C, which shows that $c'(-S) = \{\gamma\}$. By induction hypothesis it is clear that multiplication by -1 interchanges γ and β , thus $c'(S) = \{\beta\}$.

Since $c'(T) = \{\alpha\}$ by induction hypothesis one has $c'(R) = \{\gamma\}$.

(ii') If $a' > b'$, this is again case D).

While the "reduced" balance of R was (a, b) where a even, b odd, $a > b$ the "reduced" balance of $-S$ is defined as (a', b') where a' even, b' odd, $a' > b'$,

and a' and b' are easily computed as

$$a' = 2b \text{ and } b' = a - b.$$

If one takes into consideration that $n+1 = a+b$ is odd, 2 is a unit in the ring $\mathbb{Z}_{n+1}$.

By identifying the nonzero elements of $\mathbb{Z}_{n+1}$ with the integers u , $1 \leq u \leq n$, it is clear that

$$a' \equiv 2b \pmod{a+b}$$

$$b' = a - b \equiv 2a \pmod{a+b}.$$

Since $b \equiv -a \pmod{a+b}$ the transition $v : (a, b) \mapsto (a', b')$ induced

by the transition $\rho : R \rightarrow -S$ is nothing but the transition

$$(a, -a) \mapsto (-2a, 2a) \pmod{a+b}.$$

Since $a > b$, a is even and b is odd, the positive integer representing $-2a \pmod{a+b}$ is even and the positive integer representing $2a \pmod{a+b}$ is odd. Since $\text{ord}_m(-2)$ is finite, iteration will lead to a vertex $\rho^\lambda(R)$ whose reduced balance $v^\lambda(a, b) =: (a^{(\lambda)}, b^{(\lambda)})$ is such that $a^{(\lambda)} > b^{(\lambda)}$ where $a^{(\lambda)}$ is even, $b^{(\lambda)}$ is odd and $1 \leq \lambda \leq \text{ord}_m(-2)$.

$\rho^\lambda(R)$ then fulfils condition (i'), from which it is clear that

$$c'(\rho^\lambda(R)) = \{\gamma\},$$

which in turn implies $c'(\rho^{\lambda-1}(R)) = \{\gamma\}$, such that

$$c'(R) = \{\gamma\}.$$

Case E: If $a > b$, where a is odd and b is even, one has $\text{rk}(T) \leq n$:

Since T has the form $\{\sigma, \underline{y}, z\}$ where $\sigma < y < z$ one only has to consider

$$y - \sigma = 3y + z = 4y + (z - y),$$

which shows that the

$$\text{gcd}(y - \sigma, z - y) \geq \text{gcd}(y - x, z - y).$$

Since $\sigma > x$ one has $\text{rk}(T) \leq n$.

Since T is of type II and by fact 4 R is adjacent to a translate R'

of type I with the same balance then $-R'$ is of type III, whose

reduced balance is (b, a) , which is treated in case C.

Hence $c'(R') = \{\beta\}$ and $c'(R) = \{\gamma\}$.

Case F: $a < b$, a is odd, b is even.

$$T = \{\underline{y}, \sigma, z\}, \quad y < \sigma < z.$$

Again $\text{rk}(T) \leq n$ since

$$z - \sigma = 2z + 2y = 2(z - y) + 4y$$

$$\sigma - y = -3y - z = -4y + (y - z),$$

from which $\text{gcd}(\sigma - y, z - \sigma) \geq \text{gcd}(y - x, z - y)$ follows. As T is of type I

one has $c'(T) = \{\beta\}$.

Furthermore $\text{rk}(P) = \text{rk}(R) = n+1$, where $P = \{x, \underline{\tau}, z\}$. It is clear

that $x < \tau < z$. For the balance $\delta(P)$

$$z - \tau = \frac{3z + x}{2} = 2z + \frac{x - z}{2}$$

$$\tau - x = \frac{-3x - z}{2} = -2x + \frac{x - z}{2}$$

Since $4x = 3(y - x) + 2(z - y)$ it follows that $y - x \equiv 4 \pmod{8}$ and

$z - y \equiv 0 \pmod{8}$. Thus $a + b = \frac{z - x}{4}$, x and z are odd.

Thus $z-\tau \equiv 0 \pmod{4}$

and $\tau-x \equiv 0 \pmod{4}$

which implies $\text{rk}(P) = \text{rk}(R)$.

Furthermore since the reduced balance of P is

$$(a', b') = \left(\frac{\tau-x}{4}, \frac{z-\tau}{4} \right)$$

and

$$\begin{aligned} z-\tau &= \frac{3z+x}{2} \\ &\equiv z+x \pmod{a+b} \\ &\equiv -\frac{y-x}{2} \pmod{a+b}. \end{aligned}$$

Hence by considering the elements of the ring $\mathbb{Z}_{a+b}$ as the integers between 0 and $a+b-1$ one has

$$(a, b) \equiv (a, -a) \pmod{a+b}$$

and

$$(a', b') \equiv \left(\frac{a}{2}, -\frac{a}{2} \right) \pmod{a+b}.$$

By fact 4 P is adjacent to P' of type I and P'' of type III such that the balances of P, P' and P'' are identical.

One of the numbers a' and b' is odd, the other even, w.l.o.g.

a' is odd and b' is even.

(i) If $a' > b'$ one has $c'(P'') = \{\gamma\}$ by E), $c'(P') = \{\beta\}$ by C), thus $c'(P) = \{\alpha\}$ and $c'(R) = \{\gamma\}$.

(ii) If $a' < b'$ then $c'(P') = \{\beta\}$ by D) and P'' is again treated in F).

By the same argument as in D) from the finiteness of $\text{ord}_{a+b}(2)$

it follows that after finite iteration of F the situation F)(i) is obtained. $\#$

4.4.5 Corollary: Let $p \geq 23$ be a prime. Then there is no SW_3 -resolution over $\mathbb{Z}_p$.

Proof: If there is an SW_3 -resolution over $\mathbb{Z}_p$ by theorem 4.3.3 there is a resolution over $\mathbb{Z}[\frac{1}{6}]$, which when considered mod p , again would yield the given resolution over $\mathbb{Z}_p$. By theorem 4.4.4 the initial system over $\mathbb{Z}[\frac{1}{6}]$ contains the blocks

$$\{-3, -1, 2, \gamma\}$$

and

$$\{-p+2, p-1, p-3, \beta\}$$

which in $\mathbb{Z}_p$ lead to a contradiction. $\#$

Now the main theorem can be deduced almost immediately, after recalling the following famous result:

4.4.6 Theorem (F.W. Levi, B.H. Neumann): An abelian group can be ordered consistently iff it is torsionfree.

Proof: A proof can be found in Beth [8].

4.4.7 Definition: Let G be an abelian group. A multiset over G is a mapping $[M] : G \rightarrow \mathbb{N}_0$, where $M := \{x \in G \mid [M](x) > 0\}$.

Let $k \in \mathbb{N}$. A k -multiset over G is a multiset $[K]$ over G with the

property $\sum_{x \in G} [K](x) = k$.

$[K]$ may also be written in the form

$$[K] = [x_1^{\ell_1}, \dots, x_s^{\ell_s}] \quad \text{where } s \in \mathbb{N}$$

and for each $i \in \mathbb{N}_s$ $x_i \in G$, $\ell_i := [M](x_i)$ such that $\sum_{i \in \mathbb{N}_s} \ell_i = k$.

Let $\sum_{x \in [K]} x := \sum_{i=1}^s \ell_i x_i$ and let $G^{[k]}$ denote the class of all

k -multisets over G .

4.4.8 Main Theorem: Let G be an abelian group such that $6 \in \text{Aut } G$.

There exists an SW_3 -resolution over G iff G is torsionfree.

Proof: Let G be torsionfree. Then G can be ordered consistently.

Let $X = G \cup \{\alpha, \beta, \gamma\}$. Then define the initial SQS $S_0 = (X, \beta_0)$

as follows:

Let $G^{[4]}$ be the class of multisets in G with total valency 4. Let

$$G_0^{[4]} = \{[K] \in G^{[4]} \mid \sum_{k \in [K]} k = 0\}.$$

For $[K] \in G_0^{[4]}$ let $\bar{K}$ be the set of distinct elements of K .

Then β_0 is defined as follows:

Let $[K] \in G_0^{[4]}$. If

$$|\bar{K}| = 4 \text{ then } \bar{K} \in \beta_0.$$

For $|\bar{K}| = 3$ one has $\bar{K} = \{x, y, z\}$ and $x < y < z$:

$$\text{If } \begin{cases} x+2y+z = 0 \text{ let } \bar{K} \cup \{\alpha\} \in \beta_0 \\ 2x+y+z = 0 \text{ let } \bar{K} \cup \{\beta\} \in \beta_0 \\ x+y+2z = 0 \text{ let } \bar{K} \cup \{\gamma\} \in \beta_0. \end{cases}$$

If $|\bar{K}| = 2$ one has $\bar{K} = \{x, y\}$ where $x < y$.

$$\text{Then define } \begin{cases} \bar{K} \cup \{\alpha, \gamma\} \in \beta_0 \text{ if } x+3y = 0 \\ \bar{K} \cup \{\beta, \gamma\} \in \beta_0 \text{ if } 2x+2y = 0 \\ \bar{K} \cup \{\alpha, \beta\} \in \beta_0 \text{ if } 3x+y = 0. \end{cases}$$

Furthermore let $\{\alpha, \beta, \gamma, 0\} \in \beta_0$.

Since this distribution of α, β, γ corresponds to the admissible colouring of Ω^G which is completely analogous to the standard labelling,

it would only mean repeating the proof of 4.4.2 to show that

$\{\beta_0 + g \mid g \in G\}$ is an SW_3 -resolution.

In order to prove necessity, assume G is not torsionfree. Then G

has a subgroup $\mathbb{Z}_p$ for some prime p . If there were an SW_3 -resolution over G one would have an SW_3 -resolution over $\mathbb{Z}_p$ by proposition 4.2.10. By theorem 4.3.3 then there were an SW_3 -resolution over $\mathbb{Z}[\frac{1}{6}]$ such that by considering this resolution again mod p the given resolution over $\mathbb{Z}_p$ is recovered. This is impossible by corollary 4.4.5. $\#$

CHAPTER 5: HIGHER RESOLUTIONS

5.1 Definitions: In this chapter it will be shown that the SW_3 -resolution presented in chapter 4 is a special case of a general method to partition the class of all $k+1$ -subsets of an infinite (countable) set into Steiner Systems $S_1(k, k+1, |X|)$ for every $k \in \mathbb{N}$.

5.1.1 Definition: Let $k \in \mathbb{N}$ be a positive integer. Let G_k be a torsion free abelian group such that $(k+1)! \in \text{Aut } G_k$. Let $\Omega_k = \{\omega_1, \dots, \omega_k\}$ be a set of symbols disjoint from G and define $X_k := G_k \cup \Omega_k$. A partition $\{\beta_g \mid g \in G_k\}$ of $\binom{X_k}{k+1}$ is called a stratified-weight-k-resolution of $\binom{X_k}{k+1}$, abbreviated by SW_k -resolution, if

- (i) $\forall g \in G_k : \beta_g = \beta_0 + g$
- (ii) $K \in \beta_0 \cap \binom{G_k}{k+1} \Rightarrow \sum_{x \in K} x = 0$
- (iii) (X_k, β_0) is a Steiner System $S_1(k, k+1, |X_k|)$.

5.1.2 Examples:

a) $k = 1$: Let $G_1 = \mathbb{Z}[\frac{1}{2}]$ and define

$$\beta_0 = \{\{x, -x\} \mid x \in G_1\} \cup \{\{0, \omega_1\}\}.$$

b) $k = 2$: Let $G_2 = \mathbb{Z}[\frac{1}{6}]$ and define

$$\begin{aligned} \beta_0 = & \left\{ T \in \binom{G_1}{3} \mid \sum_{t \in T} t = 0 \right\} \cup \left\{ \{t, -2t, \omega_1\} \mid t < 0 \right\} \\ & \cup \left\{ \{-2t, t, \omega_2\} \mid t > 0 \right\} \cup \left\{ \{0, \omega_1, \omega_2\} \right\} \end{aligned}$$

c) $k = 3$: Let $G_3 = \mathbb{Z}[\frac{1}{6}]$ and define β_0 as given in 4.4.8.

5.1.3 Remark: The SW_1 -resolution (respectively the SW_2 -resolution)

defined in 5.1.2 clearly corresponds to the resolutions given in 2.4.7

(respectively 3.2.3) for the finite case. When discussing these cases earlier, the condition $2! \in \text{Aut } G$ (respectively $3! \in \text{Aut } G$) was automatically fulfilled, since for $k = 1$ $G = \mathbb{Z}_{2n+1}$ for some $n \in \mathbb{N}$,

and for $k = 2$ $G = \mathbb{Z}_m$, where $m \equiv 1, 5 \pmod{6}$.

5.2 The Existence of SW_k -Resolutions

In order to construct SW_k -resolutions one has to solve the main problem to distribute the symbols $\{\omega_1, \dots, \omega_k\}$ in such a way that the subsets, which above were called degenerate (respectively doubly-degenerate), i.e. the subsets of G_k which only can be made zero-sum- $k+1$ -subsets of G_k by repeating elements, are properly contained in blocks of size $k+1$ in the initial system.

In the following a convenient method for solving this problem will be presented:

5.2.1 Definition: Let k, G_k, Ω_k and X_k be as above.

Let $G_k^{[k+1]}$ be the set of $(k+1)$ -multisets in G_k

Let $\phi_k : G_k^{[k+1]} \longrightarrow (X_k^{[k+1]})$ be the following mapping:

Let $[S] = [x_1^{\ell_1}, \dots, x_s^{\ell_s}]$ be a $(k+1)$ -multiset in G_k , i.e.

$$\forall i \in \mathbb{N}_s : \ell_i \in \mathbb{N}, \sum_{i=1}^s \ell_i = k+1, \text{ where } x_1 < \dots < x_s \text{ for some consistent .}$$

order relation on G_k .

Then let

$$\phi_k([S]) := \bigcup_{i=1}^s \{x_i\} \cup \Omega_i^{[S]} \text{ where } \Omega_i^{[S]} := \{\omega_p \mid \sum_{r=1}^{i-1} \ell_r < p < \sum_{r=1}^i \ell_r\}.$$

ϕ_k is called the SW-coding of the $(k+1)$ -multisets in G_k .

5.2.2 Remark: The SW-coding is the immediate generalization of the method used by Schreiber [45] and Wilson [54] for the SW_2 -resolution in the finite case. Furthermore, the SW-coding in the case $k = 3$ is equivalent to the standard labelling.

The following example illustrates the SW-coding:

5.2.3 Example: Let $k = 10$ and $[S]$ be the 11-multiset

$[S] = [-5^3, -3^2, -1^1, 0^1, 1^1, 2^2, 3^1]$ in $\mathbb{Z}[\frac{1}{11!}]$. The SW-coding $\phi_{10}([S])$ is the 11-set $\{\omega_1, \omega_2, -5, \omega_4, -3, -1, 0, 1, \omega_9, 2, 3\}$ in X_{10} .

The elements ω_j label the positions where repeated elements occur in the linearly ordered $k+1$ -multiset. The following statement is immediate:

5.2.4 Observation: Let $k \in \mathbb{N}$. The SW-coding $\phi_k : G_k^{[k+1]} \rightarrow (X_k)_{k+1}$ is a bijection.

With these few preparations the main theorem of this chapter can be proved:

5.2.5 Theorem: Let $k \in \mathbb{N}$, $G_k = \mathbb{Z}[\frac{1}{(k+1)!}]$ and X_k, Ω_k and ϕ_k be as defined above.

Let $\Omega_0 = \{\phi_k([S]) \mid [S] \in G_k^{[k+1]}, \sum_{x \in [S]} x = 0\}$.

Then $\{\Omega_0 + g \mid g \in G_k\}$ is a SW_k -resolution of $(X_k)_{k+1}$.

Proof: Since $G_k = \mathbb{Z}[\frac{1}{(k+1)!}]$, $\{\Omega_0 + g \mid g \in G_k\}$ clearly is a partition of $(X_k)_{k+1}$.

It remains to show that (X_k, Ω_0) is a Steiner System $S_1(k, k+1, |X_k|)$.

For this purpose let R be a k -subset of X_k . $R = \{x_1, \dots, x_{k-s}, \omega_{i_1}, \dots, \omega_{i_s}\}$, where $\{x_1, \dots, x_{k-s}\} = R \cap G_k$, $x_1 < \dots < x_{k-2}$ and $i_1 < \dots < i_s$.

Let $z \in G_k$ and let $f : \mathbb{N}_{k+1} \setminus \{i_1, \dots, i_s\} \rightarrow \{x_1, \dots, x_{k-s}, z\}$ be a

surjective mapping with the property $f(i) \leq f(j)$ for all

$i, j \in \mathbb{N}_{k+1} \setminus \{i_1, \dots, i_s\}$ with $i < j$.

Define

$$R(z) = \begin{cases} R \cup \{z\} & \text{if } z \notin R \cap G_k \\ R \cup \{\omega_\rho\} & \text{if } f(\rho) = f(\tau) = z \text{ for some } \rho < \tau, \\ & \text{where } \rho, \tau \in \mathbb{N}_{k+1} \setminus \{i_1, \dots, i_s\}. \end{cases}$$

Let $[M(z)] = \phi_k^{-1}(R(z))$ and

$$\sigma(z) := \sum_{g \in [M(z)]} g$$

It is clear that σ is a strictly monotone, piecewise linear function

$\sigma : \mathbb{Z}[\frac{1}{(k+1)!}] \longrightarrow \mathbb{Z}[\frac{1}{(k+1)!}]$, which has a continuous, strictly monotone, piecewise linear extension

$$\bar{\sigma} : \mathbb{R} \longrightarrow \mathbb{R}.$$

Observe that there are constants $c^+ > 0$ and $c^- < 0$ such that for $z > c^+$ $\sigma(z) > 0$ and for $z < c^-$ $\sigma(z) < 0$.

Thus there exists a unique element $z_0 \in \mathbb{R}$ such that $\sigma(z_0) = 0$.

Since $\bar{\sigma}|_{\mathbb{Z}[\frac{1}{(k+1)!}]} = \sigma$, and the equation of the linear pieces have coefficients in $\mathbb{Z}[\frac{1}{(k+1)!}]$, while for each piece the slope is an integer m , $1 \leq m \leq k+1$ it is immediate that

$$z_0 \in \mathbb{Z}[\frac{1}{(k+1)!}]$$

and $R(z_0)$ is the unique block in $\mathcal{R}_0$ containing R .

#

NOTATIONS:

$AG(n, q)$	n -dimensional affine geometry over $GF(q)$
$\mathcal{O}_n$	alternating group of degree n
$\mathcal{O}_X$	alternating group on a set X
$GF(q)$	field of q elements, q prime power
$GF(q)^*$	$= GF(q) \setminus \{0\}$
$GF(q)^*$	$= \{x^2 \mid x \in GF(q)^*\}$
$GL(n, q)$	group of all linear automorphisms of V_q^n
$\begin{bmatrix} n \\ k \end{bmatrix}_q$	the number of k -dimensional subspaces in V_q^n
$\mathbb{N}$	positive integers
$\mathbb{N}_0$	nonnegative integers
$\mathbb{N}_n$	$= \{m \in \mathbb{N} \mid m \leq n\}$
$PG(n, q)$	n -dimensional projective geometry over $GF(q)$
$PGL(n, q)$	projective general linear group, induced by $GL(n, q)$
$\mathcal{S}_n$	symmetric group of degree n
$\mathcal{S}_X$	symmetric group on a set X
2^X	power set of a set X
V_q^n	n -dimensional vector space over $GF(q)$
$ X $	cardinality of set X
$\binom{X}{n}$	$= \{S \in 2^X \mid S = n\}, n \in \mathbb{N}$
$\mathbb{Z}$	set of integers
$\mathbb{Z}_n$	residues mod n , $n \in \mathbb{N}$, being identified canonically with the set of integers $\{z \mid 0 \leq z \leq n-1\}$.

A partition of a set X is a subset $\{B_i \mid i \in I\}$ of 2^X such that

$\bigcup_{i \in I} B_i = X$ and for any $i, j \in I$ $i \neq j$ implies $B_i \cap B_j = \emptyset$.

A mapping $\phi : X \rightarrow X$ is usually considered to be identified with its

canonical extension $\bar{\phi} : 2^X \rightarrow 2^X$. Especially if X is an abelian group

and $g \in X$ is the permutation $\pi_g : x \mapsto x+g$ of X , then for each $B \in 2^X$

$B+g := \pi_g(B) = \{b+g \mid b \in B\}$ and for each $\mathcal{B} \subset 2^X$ $\mathcal{B}+g := \{B+g \mid B \in \mathcal{B}\}$.

REFERENCES:

- [1] BAER, R.: Linear algebra and projective geometry, Academic Press, New York, 1952.
- [2] BAKER, R.: Partitioning the planes of $AG_{2m}(2)$ into 2-designs, Discrete Math., 15, 1976, 205-211.
- [3] BARANYAI, Z.: On the factorization of the complete uniform hypergraph, to appear in: Proceedings Erdős-Colloquium Keszthely.
- [4] BARLOTTI, A.: Some topics in finite geometrical structures, Institute of Statistics Mimeo Series No. 439, Chapel Hill, 1965
- [5] BEKER, H.: An orbit theorem for designs, Geom. Dedic. 5, 1976, 425-433.
- [6] BEKER, H.; PIPER, F.: Some designs which admit strong tactical decompositions, to appear
- [7] BETH, T.: Algebraische Auflösungsalgorithmen für eine unendliche Familie von 3-designs, Le Matematiche, 29, 1974, 105-135.
- [8] BETH, T.; VIJAYAN, K.S.: A combinatorial filing system based on finite groups of automorphisms, to appear in Computing
- [9] BETH, T.: Theorie der Vertretersysteme, Institut für Mathematische Maschinen und Datenverarbeitung, Erlangen 1977
- [10] BEUTELSPACHER, A.: On parallelisms in finite projective spaces, Geom. Dedic., 3, 1974, 35-40
- [11] BOSE, R.C.: On the construction of balanced incomplete block designs, Ann. Eugenics, 9, 1939, 353-399
- [12] BROUWER, A.: On associative block designs, Preprint, Mathematisch Centrum, Amsterdam, 1976
- [13] CAMERON, P.: Parallelisms of complete designs, London Math. Soc. Lect. Notes, 23, Cambridge Univ. Press, Cambridge 1976.
- [14] CAMERON, P.; VAN LINT, J.: Graph theory, coding theory and block designs, London Math. Soc. Lect. Notes 19, Cambridge Univ. Press, Cambridge 1975

- [15] CAYLEY, A.: On the triadic arrangements of seven and fifteen things, Philos. Mag. 37, 1850, 50-53.
- [16] DEMBOWSKI, P.: Finite geometries, Springer, New York 1968.
- [17] DEMBOWSKI, P.: Kombinatorik, Bibl. Inst., Mannheim 1970
- [18] DENNISTON, R.H.F.: Double resolvability of some complete 3-designs, Manuscripta Math. 12, 1974, 105-112.
- [19] DENNISTON, R.H.F.: Some packings with Steiner triple systems, Discrete Math., 9, 1974, 213-227.
- [20] DENNISTON, R.H.F.: Sylvester's problem of the fifteen school girls, Discrete Math., 9, 1974, 229-233.
- [21] DENNISTON, R.H.F.: Some new 5-designs, Bull. London Math. Soc., 8, 1976, 263-267.
- [22] DENNISTON, R.H.F.: Three doubly resolvable complete 3-designs, submitted to Manuscripta Math.
- [23] DENNISTON, R.H.F.: Further cases of double resolvability, submitted to Manuscripta Math.
- [24] DOYEN, J.; ROSA, A.: An extended bibliography and survey of Steiner systems, Math. Reports No. 92, McMaster University, 1977
- [25] FERRERO, G.: Gruppi di Steiner e sistemi fini, Le Matematiche 27, 1972, 167-190
- [26] FERRERO, G.: Sui gruppi che ammettono funzioni di Steiner, Rend. Ist. Mat. Univ. Trieste, 4, 1972, 156-170.
- [27] HALL, M. Jr.: Combinatorial Theory, Blaisdell, Waltham, 1967
- [28] HALDER, H.; HEISE, W.: Einführung in die Kombinatorik, Hanser, München 1976
- [29] HANANI, H.: On quadruple systems, Canad. J. Math., 12, 1960, 145-157.
- [30] HANANI, H.: Balanced incomplete block designs and related designs, Discrete Math. 11, 1975, 255-369.
- [31] HANANI, H.; RAY-CHAUDHURI, D.; WILSON, R.: On resolvable designs, Discrete Math. 3, 1972, 343-357.
- [32] KIRKMAN, T.: On a problem in combinations, Cambridge and Dublin Math. J., 2, 1847, 191-204

- [33] KIRKMAN, T.: Note on an unanswered prize question, Cambridge and Dublin Math. J. 5, 1850, 255-262.
- [34] KRAMER, E.; MESNER, D.: Intersections among Steiner systems, J. Comb. Th. A., 16, 1974, 273-285
- [35] KRAMER, E.; MESNER, D.: The possible (impossible) systems of 11 disjoint $S(2,3,13)$'s $[S(3,4,14)$'s] with automorphism of order 11, Utilitas Math. 7, 1975, 55-58.
- [36] LINDNER, C.; ROSA, A.: Steiner quadruple systems, preprint, June 1977
- [37] LÜNEBURG, H.: Transitive Erweiterungen endlicher Permutationsgruppen, Lecture Notes in Mathematics, No. 19, Springer, Berlin, Heidelberg, New York 1969
- [38] MACWILLIAMS, J.; SLOANE, N.: The theory of error correcting codes, North Holland, Amsterdam, to appear 1977.
- [39] MENDELSON, N.; HUNG, S.: On the Steiner systems $S(3,4,14)$ and $S(4,5,15)$. Utilitas Math., 1, 1972, 5-95.
- [40] NETTO, E.: Lehrbuch der Combinatorik, Teubner, Leipzig, 1901
- [41] PELTESOHN, R.: Das Turnierproblem für Spiele zu je dreien, Dissertation, Berlin 1936.
- [42] PELTESOHN, R.: Eine Lösung der beiden Heffterschen Differenzenprobleme, Compositio Math., 6, 1939, 251-257.
- [43] RAY-CHAUDHURI, D.; WILSON, R.: Solution of Kirkman's school girl problem, Proc. Symp. Pure Math. 19, 1971.
- [44] REISZ, M.: Über eine Steinersche combinatorische Aufgabe, welche im 45sten Bande dieses Journals, Seite 181, gestellt worden ist, J. Reine Angew. Math. 56, 1859, 326-344.
- [45] SCHREIBER, S.: Covering all triples on n marks by disjoint Steiner systems, J. Comb. Th., 15, 1973, 347-350.
- [46] SCHREIBER, S.: Some mappings of periodic groups, Israel J. Math. 17, 1974, 117-123.
- [47] SCHREIBER, S.: Some balanced complete block designs, Israel J. Math., 18, 1974, 31-37.
- [48] SLOANE, N.: A short course on error correcting codes, Springer, New York 1975.

- [49] STEINER, J.: Combinatorische Aufgabe, J. Reine Angew. Math., 45, 1853, 181-182.
- [50] SYLVESTER, J.: Proposed Problem, Educational Times, Nov. 1st, 1875, 193.
- [51] TEIRLINCK, L.: Combinatorial structures, Thesis, Vrije Universiteit Brussel, 1977
- [52] VAN LINT, J.: Coding theory, Lecture Notes in Math., No. 201, Springer, Berlin 1973.
- [53] WILSON, R.: Cyclotomy and difference families in elementary abelian groups, J. Number Theory, 4, 1972, 17-47.
- [54] WILSON, R.: Some partitions of all triples into Steiner triple systems, Lecture Notes in Math. No. 411, Springer, Berlin 1974, 267-277.
- [55] WILSON, R.: An existence theory for pairwise balanced designs III, J. Comb. Th. (A), 18, 1975, 71-79.
- [56] WITT, E.: Die 5-fach transitiven Gruppen von Mathieu, Abh. Math. Sem. Univ. Hamburg, 12, 1938, 256-264.
- [57] WITT, E.: Über Steinersche Systeme, Abh. Math. Sem. Univ. Hamburg, 12, 1938, 265-275.

Lebenslauf

16.11.1949 in Hannover geboren

1956- 1960 Besuch der Volksschule in Seelze (Hannover)

1960- 1968 Besuch des Gymnasiums Goetheschule in Hannover

11.6.1968 Abitur

1.10.1968 Immatrikulation an der Universität Göttingen

21.10.1970 Diplomvorprüfung in Mathematik an der Universität
Göttingen

9.7.1973 Diplomhauptprüfung in Mathematik an der
Universität Göttingen

1973- 1974 DAAD-Stipendiat an der Ohio State University,
Columbus, Ohio, USA

seit 1.7.1974 Verwalter der Dienstgeschäfte eines wissenschaft-
lichen Assistenten am Institut für Mathematische
Maschinen und Datenverarbeitung der Universität
Erlangen

seit 1974 verheiratet, zwei Töchter

Thomas Beth

In letzter Zeit sind folgende Arbeitsberichte des Instituts
für Mathematische Maschinen und Datenverarbeitung erschienen :
=====

Band 9
=====

- NR. 1 Brendel, W., Frühauf, T., Nagl, M. :
Graph Rewriting Systems II.
Three Papers on Theory, Application, and Implementation.
(Februar 1976)
- NR. 2 Brüggmann, H. W., Rudert, A., Lehr, H. :
EBIS
Strukturierte Bildprogrammierung auf höherer Ebene.
(Februar 1976)
- NR. 3 Hofmann, W., Wichmann, H. :
Konzept der Vertikalverarbeitung.
Implementierung und Analyse vertikaler Algorithmen
auf einem mikroprogrammierten Rechner.
(Mai 1976)
- NR. 4 Jordan, H. F., Smith, B. J. :
The Hardware-Software Interface.
(Juni 1976)
- NR. 5 Gernoth, B., Schmidt, B. :
Das Modell MEM-SIM.
Beschreibung eines Simulationsmodells zur Unter-
suchung einer Rechenanlage mit einer symmetrischen
Mehrprozessorkonfiguration und privaten Speichern.
(Oktober 1976)
- NR. 6 Grötsch, E. :
Vergleichende Studie über parallele Ersetzung
markierter Graphen.
Jahn, B. :
Eine Studie zur Implementierung von Graph-Grammatiken
unter Verwendung von Assoziativverarbeitung.
(Dezember 1976)
- NR. 7 Mertens, P., Neuwirth, W., Purucker, G.,
Schaller, K., Schmitt, W. :
Verknüpfung von Daten- und Methodenbanken, dargestellt
am Beispiel der Analyse von Marktforschungsdaten.
(Dezember 1976)
- NR. 8 Parallelismus in der Informatik.
Wissenschaftliches Kolloquium aus Anlass des Zehnjährigen
Bestehens des IMMD, Erlangen, 10./11. Juni 1976.
(Dezember 1976)
- NR. 9 Jahresbericht 1976 der Informatik.
(März 1977)

and 10
=====

- NR. 1 Hoffmann, W. :
Modelle und Analysen von Teilnehmerrechensystemen,
angewendet auf das Teilnehmersystems RESPOND unter
CD 3300 MASTER.
(Februar 1977)
- NR. 2 Körber, K., Werzinger, G. :
Das Modell SIM-LAB.
Simulation eines klinisch-chemischen Laboratoriums.
(März 1977)
- NR. 3 Altmann, W., Weber, D. :
Programmierungsmethodik.
(März 1977)
- NR. 4 Maehle, E. :
Fehlertolerante Rechnerstrukturen.
(April 1977)
- NR. 5 Beth, T. :
Kombinatorik: Theorie der Vertretersysteme.
(April 1977)
- NR. 6 Mertens, P. :
Einige Hinweise zur technischen Gestaltung von
Bildschirmdialogen.
(Mai 1977)
- NR. 7 Jäpel, D. :
Ein Begriffssystem zur Formulierung von Schutzaspekten
und seine Anwendung auf Programmsysteme.
(Juni 1977)
- NR. 8 Brendel, W., Grötsch, E., Nagl, M., Schneider, H.-J. :
Graphersetzungssysteme, Beiträge zur Theorie, Anwen-
dung und Implementierung.
(Juni 1977)
- NR. 9 Rüdell, W. :
Darstellung und Vergleich abstrakter Modelle zur
Beschreibung geschützter Systeme.
(Juli 1977)
- NR. 10 Bolch, G., Gall, R., Grassl, M., Schmidt, B. :
Modelle für Trommelspeicher.
(Juli 1977)
- NR. 11 v. Eichhorn, K. :
Steiner Systeme, Codes und affine Räume.
(Juli 1977)
- NR. 12 Göttler, H. :
Zweistufige Graphmanipulationssysteme für die
Semantik von Programmiersprachen.
(Juli 1977)

and 10 (Forts.)
=====

- NR. 13 Keramidis, S. :
Ein allgemeines formales Modell für Betriebs-
systeme und dessen Implementierung.
(September 1977)
- NR. 14 Arnold, F., Benker, L., Grütz, M. :
Die Fast Fourier Transformation und Möglich-
keiten ihrer Implementierung auf EGPA.
(November 1977)
- NR. 15 Gardill, R., Händler, W., Hessling, H.,
Klar, R., Spies, P. P. :
ERES
Eine nichtprozedurale Rechnerentwurfssprache
mit präziser Zeitbeschreibung.
(November 1977)
- NR. 16 Wichmann, H. :
Entwicklung und Bewertung von Algorithmen für
ein mikroprogrammiertes Parallel- und Assoziativ-
konzept auf Mikroprogramm- und Benutzerebene.
(Dezember 1977)
- NR. 17 Brügmann, H. W. :
EBIDIS - Strukturierte Bildprogrammierung im Dialog.
(Dezember 1977)
- NR. 18 Jahresbericht 1977 der Informatik.
(März 1978)

and 11

=====

- NR. 1 Körber, K., Werzinger, G. :
Das Modell SIM-LAB.
Beschreibung des Grundmodells.
(Februar 1978)
- NR. 2 Körber, K., Werzinger, G. :
Das Modell SIM-LAB.
Beschreibung der Modellerweiterungen und der Strategien.
(Februar 1978)
- NR. 3 Körber, K., Werzinger, G. :
Das Modell SIM-LAB.
Listing der Quellprogramme.
(Februar 1978)
-

Offsetdruck-Fotodruck

J. Hegl, 8520 Erlangen, Hauptstr. 109 (Nähe Martin-Luther-Platz) Tel. 22990